THE INTERNET WILL NOT BREAK: DENYING BAD SAMARITANS § 230 IMMUNITY

Danielle Keats Citron and Benjamin Wittes***

INTRODUCTION

The social media site Omegle sports the jaunty slogan, "Talk to strangers!"[1] The site's front page announces that it is "a great way to meet new friends. When you use Omegle, we pick someone else at random and let you talk one-on-one."[2]

Omegle is not exactly a social media site for sexual predators, but it is fair to say that a social network designed for the benefit of the predator community would look a lot like Omegle. The site itself seems to understand this. The opening paragraph—the same one in which the site proclaims itself a great way to meet new friends—warns that "[p]redators have been known to use Omegle, so please be careful."[3] The site's legal disclaimer, also on its front page, specifically warns: "Understand that human behavior is fundamentally uncontrollable, that the people you encounter on Omegle may not behave appropriately, and that *they are solely responsible for their own behavior*. Use Omegle at your own peril."[4] As to Omegle's video chat, the site warns: "Omegle video chat is moderated. However, moderation is not perfect. You may still encounter people who misbehave. They are *solely responsible for their own behavior*."[5]

---

* Morton & Sophia Macht Professor of Law at the University of Maryland Francis King Carey School of Law. We are grateful to Antigone Davis, Mary Anne Franks, Carrie Goldberg, Eric Goldman, Brittan Heller, Daphne Keller, Kate Klonick, Jonathan Mayer, and Alexander Tsesis for their feedback as well as to the participants in the Hoover Institution's conference on the power of platforms and the Department of Justice, Computer Crimes and Intellectual Property Cyber Crime section's symposium. We are grateful to Susan McCarty and Jennifer Smith for their research help. Much thanks to the *Fordham Law Review* and Alexander Tsesis for hosting the *Terrorist Incitement on the Internet* symposium and including us in this volume. Serious thanks to our editors Deema Nagib and Julia MacAllister for their helpful comments. For an overview of the *Fordham Law Review* symposium, see Alexander Tsesis, *Foreword: Terrorist Incitement on the Internet*, 86 FORDHAM L. REV. 367 (2017).
** Editor-in-Chief, *Lawfare*; Senior Fellow in Governance Studies, Brookings Institution.

1. OMEGLE, http://www.omegle.com/ [https://perma.cc/4UQB-97XY] (last visited Oct. 16, 2017).
2. *Id.*
3. *Id.*
4. *Id.* (emphasis added).
5. *Id.* (emphasis added).

Omegle's disclaimer of responsibility for its users' "misbehavior" might sound like magical thinking. After all, the site has specifically warned young users that Omegle might be pairing them with sexual predators for one-on-one chats. But, however absurd the claim may seem, the site is accurately describing its immunity from liability for whatever happens. Under the prevailing interpretation of § 230 of the Communications Decency Act (CDA), the site's users—even sexual predators preying on children—are "solely responsible for their own behavior."[6] No matter that the site was clear eyed that its service might be putting sexual predators in contact with children. As most courts have understood the statute, Omegle would enjoy broad immunity from liability arising from user-generated content.[7] This would probably be true even if Omegle changed its slogan to "Forbidden Fun with Boys and Girls!"

The Dirty is a site devoted to spreading gossip, often about college students. The site's founder, Nik Richie, has encouraged readers to email him "dirt" on people they know.[8] Richie pastes his favorite emails in blog posts, often alongside images showing ordinary people "scantily clad, inebriated, and unfaithful."[9] Posts have led to a torrent of abuse, with commenters accusing the subjects of "dirt" of having sexually transmitted infections, psychiatric disorders, and financial problems.[10] Richie has admittedly "ruin[ed] people sometimes out of fun."[11] That admission is not against interest—Richie knows well that he cannot be sued for his role in the abuse because what users do is on them. Courts applying § 230's immunity provision have dismissed efforts to hold Richie responsible for defamatory posts that have damaged lives and careers.[12]

Now consider the relationship between social media companies and terrorist groups. Last year, one of us (Wittes) undertook a survey of overseas groups that were formally designated as foreign terrorist groups, yet still had active social media accounts.[13] Federal law allows civil and criminal penalties for providing material support—including anything of value—to

---

6. *Id.*

7. As we explore in this piece, a handful of cases have refused to immunize providers from liability because they were not being sued for having published user-generated content but rather for failing to warn about a specific threat. *See, e.g.*, Doe v. Internet Brands, 824 F.3d 846, 851 (9th Cir. 2016).

8. Kate Knibbs, *Cleaning Up the Dirty*, RINGER (Apr. 19, 2017), https://www.theringer.com/the-dirty-nik-richie-gossip-site-relaunch-4a086aa24536 [http://perma.cc/875R-RMLW].

9. *Id.*

10. Kashmir Hill, *The Dirty Business: How Gossipmonger Nik Richie Stays Afloat*, FORBES (Nov. 11, 2010), https://www.forbes.com/sites/kashmirhill/2010/11/11/the-dirty-business-how-gossipmonger-nik-richie-of-thedirty-com-stays-afloat/ [http://perma.cc/HQ77-R69C].

11. Knibbs, *supra* note 8.

12. *See, e.g.*, Dyer v. Dirty World, LLC, No. CV-11-0074-PHX-SMM, 2011 WL 2173900, at *1 (D. Ariz. June 2, 2011).

13. *See* Zoe Bedell & Benjamin Wittes, *Tweeting Terrorists, Part I: Don't Look Now but a Lot of Terrorist Groups Are Using Twitter*, LAWFARE (Feb. 14, 2016), https://www.lawfareblog.com/tweeting-terrorists-part-i-dont-look-now-lot-terrorist-groups-are-using-twitter [http://perma.cc/2TUV-K6EB].

designated foreign terrorist groups.[14] Yet numerous designated terrorist groups, including Hamas, Hezbollah, the PKK, and Lakshar-e-Taiba, openly maintained an online presence on well-known social media services, including Facebook and Twitter;[15] several of those accounts were suspended after publication of Wittes's article.[16] Yet because of § 230's immunity provision, efforts to hold social media companies responsible under the civil provisions of the federal material-support statute have consistently failed.[17]

We offer the modest proposition that § 230 immunity is too sweeping. In physical space, a business that arranged private rooms for strangers to meet, knowing that sexual predators were using its service to meet kids, would have to do a great deal more than warn people to proceed "at their own peril" to avoid liability when bad things happened. A physical magazine devoted to publishing user-submitted malicious gossip about nonpublic figures would face a blizzard of lawsuits as false and privacy-invading materials harmed people's lives. And a company that knowingly allowed designated foreign terrorist groups to use their physical services would face all sorts of lawsuits from victims of terrorist attacks. Something is out of whack—and requires rethinking—when such activities are categorically immunized from liability merely because they happen online.

This was not, as highlighted below, what Congress had in mind in 1996 when it adopted the CDA. The CDA was part of a broad campaign—rather ironically in retrospect—to restrict access to sexually explicit material online.[18] Lawmakers thought they were devising a limited safe harbor from liability for online providers engaged in self-regulation. Because regulators could not keep up with the volume of noxious material online, the participation of private actors was essential.[19]

Courts, however, have extended this safe harbor far beyond what the provision's words, context, and purpose support.[20] Lower courts have ironically applied § 230, entitled "[p]rotection for private blocking and screening of offensive material," to immunize from liability sites designed to purvey offensive material.[21] The CDA's origins in the censorship of "offensive" material and protections against abuse are inconsistent with outlandishly broad interpretations that have served to immunize platforms dedicated to abuse and others that deliberately host users' illegal activities.

---

14. *See* 18 U.S.C. § 2339B (2012).

15. Bedell & Wittes, *supra* note 13.

16. Selena Larson, *Twitter Suspends 377,000 Accounts for Pro-Terrorism Content*, CNN (Mar. 21, 2017, 3:02 PM), http://www.money.cnn.com/2017/03/21/technology/twitter-bans-terrorism-accounts/index.html [https://perma.cc/Q66L-XWPE].

17. *See, e.g.*, Cohen v. Facebook, Inc., 16-CV-4453, 2017 WL 2192621, at *1 (E.D.N.Y. May 18, 2017) (dismissing claims based on the federal material-support statute against Facebook because failure to remove Hamas postings concerned the defendant's role as a publisher of online content and thus fell within § 230(c)(1)'s immunity provision); Fields v. Twitter, Inc., 200 F. Supp. 3d 964, 971–72 (N.D. Cal. 2016).

18. S. REP. NO. 104-23, at 59 (1995).

19. 141 CONG. REC. H8469–70 (daily ed. Aug. 4, 1995) (statement of Rep. Cox).

20. Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 116 (2009).

21. *Id.* (quoting 47 U.S.C. § 230 (2012)).

Section 230 is overdue for a rethinking. If courts do not construe the scope of federal immunity to avoid injustice, we argue, Congress should amend the law. This is not to discount the important role that the immunity provision has played over the past twenty years.[22] Far from it. Section 230 immunity has enabled innovation and expression beyond the imagination of the operators of early bulletin boards and computer service providers the provision was designed to protect.

But its overbroad interpretation has left victims of online abuse with no leverage against site operators whose business models facilitate abuse. This state of affairs can be changed without undermining free expression and innovation. Broad protections for free speech and clear rules of the road are important for online platforms to operate with confidence. Section 230, at least as it is currently understood, is not necessary for either of these. With modest adjustments to § 230, either through judicial interpretation or legislation, we can have a robust culture of free speech online without shielding from liability platforms designed to host illegality or that deliberately host illegal content.

I. ORIGIN STORY: WHAT SECTION 230 WAS MEANT TO DO

The CDA, part of the Telecommunications Act of 1996, was by no stretch of the imagination a libertarian enactment.[23] It consisted of a broad attack on sexually explicit material disseminated through various media.[24] Indeed, it strayed so far from libertarian values that the U.S. Supreme Court in a landmark First Amendment case struck down several of its provisions.[25] When the CDA addressed private actors, as it did in § 230, it was not to give them impunity for helping third parties abuse each other. Rather, it sought "to encourage telecommunications and information service providers to deploy new technologies and policies" to block or filter offensive material.[26]

To understand what Congress was trying to do when it passed § 230, it is helpful to start with the case that prompted its adoption: *Stratton Oakmont*,

22. DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 171 (2014).

23. *Id.*; *see also* Citron, *supra* note 20, at 116 (exploring the CDA generally and § 230 specifically).

24. *See* S. REP. NO. 104-23, at 59 (1995).

25. *See* Reno v. ACLU, 521 U.S. 844, 865 (1997); *see also* United States v. Playboy Entm't Grp., 529 U.S. 803, 827 (2000). In *Reno*, the U.S. Supreme Court struck down provisions of the CDA that criminalized the "knowing" transmission of obscene or indecent messages to underage recipients. *Reno*, 521 U.S. at 849. Internet expression, the Court explained, was too important to be limited only to what is fit for children. *Id.* at 875. The Court struck down those parts of the CDA as violations of the freedom of speech protected by the First Amendment. *Id.*

26. S. REP. NO. 104-23, at 59. As Representative Cox put it, the CDA would

> protect computer Good Samaritans, online service providers, anyone who provides a front end to the Internet, let us say, who takes steps to screen indecency and offensive material for their customers. . . . It will protect them from taking on liability such as occurred in the *Prodigy* case in New York that they should not face for helping us and for helping us solve this problem.

141 CONG. REC. H8470 (daily ed. Aug. 4, 1995) (statement of Rep. Cox) (emphasis added).

Inc. v. Prodigy Services Co.[27] Prodigy, an early online service provider, used software to filter profanity in the hopes that it would attract families to its services.[28] A user of Prodigy's services posted defamatory comments about a securities firm on a financial bulletin board. The firm sued Prodigy, arguing that it was strictly liable as the publisher of the defamation.[29] Prodigy responded that it could not possibly edit the thousands of daily messages posted to its bulletin boards as a traditional publisher would.[30] The trial court sided with the financial firm to the tune of $200 million.[31] The coup de grâce was that Prodigy lost its protection as a distributor and gained liability as a publisher because it had tried to remove objectionable material but had done so incompletely.[32]

The *Prodigy* decision caught the attention of lawmakers who wanted as much "indecent" material as possible removed from the internet so it would be safe for children.[33] The court's somewhat perverse reliance on Prodigy's filtering efforts to establish its liability for defamation (of which it had no idea) sufficiently disturbed Congress to move legislators to act to immunize such activity.[34] The concern was that holding online service providers liable for inexact screening would not result in improved screening but rather in no screening at all.[35] This is because providers could avoid publisher liability if they acted as purely passive conduits. This possibility was antithetical to lawmakers' belief that controlling the volume of noxious material online exceeded the capacity of public regulatory agencies.[36] As lawmakers saw it, self-regulation was essential to tackling objectionable content.[37]

In 1995, Senators J. James Exon and Slade Gorton introduced the CDA.[38] Under existing law, common carriers were exempt from liability if they acted in good faith to restrict obscene material.[39] The Senate committee's bill extended this immunity to online service providers to incentivize the

27. No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).
28. *Id.* at *2.
29. *Id.*
30. *Id.* at *3.
31. *See* CITRON, *supra* note 22, at 169.
32. *Prodigy*, 1995 WL 323710, at *1.
33. As Representative Bob Goodlatte explained:

> Currently, however, there is a tremendous disincentive for online service providers to create family friendly services by detecting and removing objectionable content. These providers face the risk of increased liability where they take reasonable steps to police their systems. A New York judge recently sent the online services the message to stop policing by ruling that Prodigy was subject to a $200 million libel suit simply because it did exercise some control over profanity and indecent material.

141 CONG. REC. H8471 (daily ed. Aug. 4, 1995) (statement of Rep. Goodlatte).
34. *See* Citron, *supra* note 20, at 116 n.377.
35. *See id.*
36. 141 CONG. REC. H8469–70 (daily ed. Aug. 4, 1995) (statement of Rep. Cox); *see also* Citron, *supra* note 20, at 116 n.377 (discussing the history of § 230's adoption and the goal of its drafters).
37. *See* Citron, *supra* note 20, at 116 n.377.
38. CITRON, *supra* note 22, at 171.
39. 47 U.S.C. § 223(c)(2) (2012).

adoption of new technologies and policies that would restrict access to offensive material.[40]

In the House of Representatives, Christopher Cox and Ron Wyden offered an amendment providing immunity from liability for online service providers that restricted access to objectionable material.[41] The House Rules Committee, which allowed consideration of the Cox-Wyden amendment, described that provision as "protecting from liability those providers and users seeking to clean up the Internet."[42]

The final version of § 230 of the CDA reflects this policy objective, not a broader objective of immunizing platforms for destructive third-party content they encourage or intentionally tolerate. Entitled "[p]rotection for private blocking and screening of offensive material," § 230 codifies the Cox-Wyden Amendment.[43] Section 230(c)(1) addresses the problem of underscreening, exemplified by Prodigy, by providing that, "[n]o provider or user of . . . interactive computer service[s] shall be treated as the publisher or speaker of any information provided by another information content provider."[44] Section 230(c)(2) specifies broad protections for overscreening:

> No provider or user of an interactive computer service shall be held liable on account of . . . any action voluntarily taken in good faith to restrict access to . . . 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.[45]

Section 230(e)(3) preempts contrary state laws but does not "prevent any State from enforcing any State law that is consistent with this section."[46] Federal criminal law, intellectual property law, and the Electronic Communications Privacy Act are not covered by the immunity provision.[47]

II. FORTRESS BUILT IN THE COURTS

From these humble beginnings, courts have built a mighty fortress protecting platforms from accountability for unlawful activity on their systems—even when they actively encourage such activity or intentionally

40. S. 652, 104th Cong. § 402(d)(3) (1995). Senator Exon included similar language in a floor amendment that the Senate accepted before passing the bill. *See* 141 CONG. REC. S8386 (daily ed. June 14, 1995) (statement of Sen. Exon).

41. H.R. REP. NO. 104-223, at 3 (1995); *see also supra* note 26. Representative Danner found the Cox-Wyden Amendment "a reasonable way to provide those providers of the information to help them self-regulate themselves without penalty of law." 141 CONG. REC. H8470 (daily ed. Aug. 4, 1995) (statement of Rep. Danner).

42. H.R. REP. NO. 104-223, at 3 (emphasis added).

43. 47 U.S.C. § 230(c)(1). Section 502 of the final legislation contained the Senate's additions to 47 U.S.C. § 223. Section 509 contained the House's new section, 230. *See* Pub. L. No. 104-104, § 509, 110 Stat. 133, 137 (1996). *See generally* H.R. REP. NO. 104-458 (1996) (Conf. Rep.).

44. 47 U.S.C. § 230(c)(1). The conference report described the provision as securing immunity for "Good Samaritans" engaged in blocking or filtering of objectionable content online. H.R. REP. NO. 104-458, at 193.

45. 47 U.S.C. § 230(c)(2).

46. *Id.* § 230(e)(3).

47. *Id.* § 230(e).

refuse to address it. The Supreme Court has declined to weigh in on the meaning of § 230, but state and lower federal courts have reached a "near-universal agreement" that it should be construed broadly.[48]

Courts attribute a broad-sweeping approach to the fact that "First Amendment values [drove] the CDA."[49] As one court recently put it, "Congress did not sound an uncertain trumpet when it enacted the CDA, and it chose to grant broad protections to internet publishers."[50] For support, courts have pointed to § 230's "findings" and "policy" sections, which highlight the importance of the "vibrant and competitive free market that presently exists" for the internet and the internet's role facilitating "myriad avenues for intellectual activity."[51] As Mary Anne Franks has underscored, Congress' stated goals also included the

> development of technologies that "maximize user control over what information is received" by Internet users, as well as the "vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking and harassment by means of computer." In other words, the law [wa]s intended to promote and protect the values of privacy, security and liberty alongside the values of open discourse.[52]

The plain reality is that the "core policy of § 230(c)(1)" was to protect "'Good Samaritan' blocking and screening of offensive material."[53] The

48. Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 18 (1st Cir. 2016) (citing cases from the First, Fifth, Ninth, and Eleventh Circuits), *cert. denied*, 137 S. Ct. 622 (2017) (No. 16-276).

49. *Id.* at 29.

50. *Id.*

51. *See, e.g.*, Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1099 (9th Cir. 2009) (relying on §§ 230(a)(3) and 230(b)(2) for the proposition that free speech values underlie immunity provision). Section 230(b)(2) declared it federal policy to preserve "vibrant and competitive free market that presently exists for the Internet and other interactive computer *services*, unfettered by Federal or State regulation." 47 U.S.C. § 230(b)(2). Although this section has been invoked to support the proposition that no rules should constrain the internet, a close reading shows that it refers to the marketplace of services, not the figurative marketplace of ideas. Congress did not want the FCC or the states to regulate internet access fees.

52. Mary Anne Franks, *The Lawless Internet? Myths and Misconceptions About CDA Section 230*, HUFFINGTON POST (Feb. 17, 2014), http://www.huffingtonpost.com/mary-anne-franks/section-230-the-lawless-internet_b_4455090.html [https://perma.cc/GGV8-EE7F] (quoting 47 U.S.C. § 230). Regrettably, federal stalking and harassment laws have not been enforced as vigorously as Congress hoped, though recent efforts by the Department of Justice's Computer Crimes and Intellectual Property section (CCIPs) signal an important shift in that effort. *See, e.g.*, Kenneth A. Blanco, Acting Assistant Attorney Gen., Dep't of Justice, Keynote Address at the University of Maryland Francis King Carey School of Law Symposium: When Cybercrime Turns Violent and Abusive (Sept. 15, 2017); *see also* Citron, *supra* note 20, at 83–90; Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 402 (2009). For instance, the exceptional federal prosecutor Mona Sedky of CCIPs has devoted significant energy and time combating cyberstalking and sextortion—her work should be emulated across the country. *See* Kashmir Hill, *The Cyber Prosecutor Sending Nude-Photo Thieves to Prison*, FORBES (July 31, 2014), https://www.forbes.com/sites/kashmirhill/2014/07/31/federal-prosecutor-nude-photo-hackers/ [http://perma.cc/2B7R-3KMF] (discussing the prosecutorial efforts of Wesley Hsu); *The Lawfare Podcast: Mona Sedky and Benjamin Wittes on Prosecuting Sextortion*, LAWFARE (June 25, 2016), https://www.lawfareblog.com/lawfare-podcast-mona-sedky-prosecuting-sextortion [http://perma.cc/262G-KSLV].

53. Doe v. Internet Brands, Inc., 824 F.3d 846, 851–52 (9th Cir. 2016).

judiciary's long insistence that the CDA solely reflected "Congress' desire to promote unfettered speech on the Internet"[54] so ignores its text and history as to bring to mind Justice Antonin Scalia's admonition against selectively determining legislative intent in the manner of someone at a party who "look[s] over the heads of the crowd and pick[s] out [their] friends."[55]

A. Breadth of the Immunity

We recognize that the language of § 230(c)(1) is, by its terms, broad. It does not, after all, explicitly limit the liability shield it creates to those companies that actually engage in some measure of Good Samaritan blocking or screening. While the intent of the provision—to make sure that companies that do some measure of blocking are immunized for the stuff they miss in § 230(c)(1) and are immunized for the act of blocking itself in § 230(c)(2)—is clear from history and context, the language of 230(c)(1) admittedly sweeps more broadly than that, reaching online service providers more generally.

But even with that recognition, the broad construction of the CDA's immunity provision adopted by the courts has produced an immunity from liability that is far more sweeping than anything the law's words, context, and history support.[56] Platforms have been protected from liability even though they republished content knowing it might violate the law,[57] encouraged users to post illegal content,[58] changed their design and policies for the purpose of enabling illegal activity,[59] or sold dangerous products.[60]

---

54. Zeran v. Am. Online, Inc., 129 F.3d 327, 334 (4th Cir. 1997).

55. ANTONIN SCALIA, A MATTER OF INTERPRETATION: FEDERAL COURTS AND THE LAW 36 (1997).

56. *See, e.g.*, GoDaddy.com, LLC v. Toups, 429 S.W.3d 752, 762 (Tex. App. 2014); CITRON, *supra* note 22, at 171. Courts have narrowly construed when platforms fall outside § 230's safe harbor because they cocreated content. *See* Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1167–68 (9th Cir. 2008). Only platforms that "materially contribut[e]" to content's development, such as by paying for it or requiring users to post it, are ineligible for the safe harbor. *Id.*; *see also* FTC v. Accusearch, Inc., 570 F.3d 1187, 1192, 1199 (10th Cir. 2009).

57. *See, e.g.*, Shiamili v. Real Estate Grp. of N.Y., Inc., 952 N.E.2d 1011, 1019 (N.Y. 2011); Phan v. Pham, 105 Cal. Rptr. 3d 791, 795 (Ct. App. 2010) (extending § 230 immunity to a defendant who forwarded a defamatory email and added that "[e]verything will come out to the daylight").

58. *See, e.g.*, Jones v. Dirty World Entm't Recordings LLC, 755 F.3d 398, 415–16 (6th Cir. 2014) (rejecting the plaintiff's contention that soliciting gossip constituted codevelopment of illegal content); S.C. v. Dirty World, LLC, No. 11-CV-00392-DW, 2012 WL 3335284, at *4 (W.D. Mo. Mar. 12, 2012) ("[M]erely encouraging defamatory posts is not sufficient to defeat CDA immunity.").

59. *See* Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 24 (1st Cir. 2016) (finding that Backpage was immune from liability for displayed advertising, which allegedly encouraged human trafficking), *cert. denied*, 137 S. Ct. 622 (2017) (No. 16-276).

60. *See, e.g.*, Hinton v. Amazon.com.dedc, LLC, 72 F. Supp. 3d 685, 687, 690 (S.D. Miss. 2014) (dismissing the § 230 claim because "claims against eBay arise or 'stem[] from the [] publication of information [on www.ebay.com] created by third parties'" (alterations in original) (quoting Doe v. Myspace, Inc., 528 F.3d 413, 418 (5th Cir. 2008))).

As a result, hundreds of decisions have extended § 230 immunity, with comparatively few denying or restricting it.[61]

Consider *Jane Doe No. 1 v. Backpage.com, LLC*.[62] Sex-trafficking victims sued Backpage—a classifieds hub hosting "80 percent of the online advertising for illegal commercial sex in the United States."[63] Plaintiffs alleged that Backpage did not enjoy § 230 immunity because it had deliberately structured its service to enable sex trafficking.[64] Evidence showed that the defendant had selectively removed postings discouraging sex trafficking and tailored its rules to protect the practice from detection, including anonymized email and photographs stripped of metadata.[65] Nonetheless, the court held that Backpage enjoyed immunity from liability, even as it recognized that plaintiffs' evidence was "persuasive."[66] The court reasoned that "[s]howing that a website operates through a meretricious business model is not enough to strip away those protections."[67]

Neither the text of the statute nor its history requires sweeping immunity from liability for sites like Backpage. It was, after all, part of the Communications Decency Act. Section 230 of the CDA was by no means meant to immunize services whose business is the active subversion of online decency—businesses that are not merely failing to take "Good Samaritan" steps to protect users from online indecency but are actually being "Bad Samaritans."

Granting immunity to platforms designed in part or in whole for illegal activity would seem absurd to the CDA's drafters. As Judge Frank Easterbrook noted in a case involving an alleged violation of fair housing laws, such an expansive interpretation does not harmonize with the "[d]ecency" name of the CDA because broad protection induces online computer services to "do nothing about the distribution of indecent and offensive materials."[68]

In the technology world, § 230 of the CDA is a kind of sacred cow—an untouchable protection of near-constitutional status.[69] It is, in some circles anyway, credited with having enabled the development of the modern

61. *See* Ambika Doran & Tom Wyrwich, *Section 230 of the Communications Decency Act Turns 20*, LAW360 (Sep. 7, 2016, 12:27 PM), https://www.law360.com/articles/836281/section-230-of-the-communications-decency-act-turns-20 [http://perma.cc/4P5P-4FF7].

62. 817 F.3d 12 (1st Cir.), *cert. denied*, 137 S. Ct. 622 (2017). For another example of increasing § 230 immunity, see Backpage.com, LLC v. McKenna, 881 F. Supp. 2d 1262, 1286–87 (W.D. Wash. 2012) (granting a preliminary injunction to prevent enforcement of a new law that may hold third-party websites liable for human trafficking).

63. Petition for Writ of Certiorari at 7, *Backpage*, 137 S. Ct. 622 (No. 16-276), 2016 WL 4610982.

64. *Backpage*, 817 F.3d at 16.

65. *Id.* at 20.

66. *Id.* at 29.

67. *Id.*

68. Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 670 (7th Cir. 2008).

69. *CDA 230: The Most Important Law Protecting Internet Speech*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/cda230 [http://perma.cc/WU2E-AWDE] (last visited Oct. 16, 2017).

internet.[70] We are not convinced that courts' sweeping departure from the law's words, context, and purpose has been the net boon for free expression that the law's celebrants imagine. The free expression calculus devised by the law's supporters often fails to consider the loss of voices in the wake of destructive harassment encouraged or tolerated by platforms.[71] We suspect that the many benefits that the immunity has enabled could have been secured at a slightly lesser price.[72]

But now that twenty years have passed, the question is whether the internet will break if § 230 is no longer accorded a broad-sweeping interpretation. Section 230's most fervent supporters argue that it is "responsible for the 'extraordinary Internet boom'" and its evisceration would sound the death knell to innovation.[73] To the extent the internet needed a broad liability shield when it was young, it certainly needs it no longer. Innovation on online platforms can at this point coexist with an expectation that platform companies will behave according to some enforceable standard of conduct.

Be that as it may, absent a Supreme Court intervention, the ship may have sailed in regards to the judiciary's interpretation of the current statute. Numerous federal courts of appeals have considered § 230, and so far anyway, the courts are in near-unanimous agreement that it conveys protection from liability far in excess of what we think constitutes reasonable public policy.[74]

---

70. *See, e.g.*, Eric Goldman, *Online User Account Termination and 47 U.S.C. § 230(c)(2)*, 2 U.C. IRVINE L. REV. 659, 671–72 (2012); Christopher Zara, *The Most Important Law in Tech Has a Problem*, WIRED (Jan. 3, 2017), https://www.wired.com/2017/01/the-most-important-law-in-tech-has-a-problem/ [http://perma.cc/723M-RBJN].

71. MAEVE DUGGAN, PEW RESEARCH CTR., ONLINE HARASSMENT IN FOCUS 2017, at 31 (2017), http://www.pewinternet.org/2017/07/11/online-harassment-2017/ [https://perma.cc/F3U2-FW7L] (finding that 42 percent of people experiencing severe harassment were "more likely to say they changed their username or deleted their profile, stopped attending offline venues or reported the incident to law enforcement"); *see* Danielle Keats Citron, *Civil Rights in Our Information Age*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 31, 33–34 (Saul Levmore & Martha Nussbaum eds., 2010).

72. Free speech scholar Jack Balkin has assessed § 230 in a measured way:

> [Section 230] has had enormous consequences for securing the vibrant culture of freedom of expression we have on the Internet today. . . . Because online service providers are insulated from liability, they have built a wide range of different applications and services that allow people to speak to each other and make things together. Section 230 is by no means a perfect piece of legislation; it may be overprotective in some respects and underprotective in others. But it has been valuable nevertheless.

Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 434 (2009) (footnotes omitted).

73. Derek Khanna, *The Law That Gave Us the Modern Internet—and the Campaign to Kill It*, ATLANTIC (Sept. 12, 2013) (quoting Eric Goldman, *Why the State Attorneys General's Assault on Internet Immunity Is a Terrible Idea*, FORBES (June 27, 2013 10:44 AM), https://www.forbes.com/sites/ericgoldman/2013/06/27/why-the-state-attorneys-generals-assault-on-internet-immunity-is-a-terrible-idea/ [https://perma.cc/UU2J-MZWQ]), https://www.theatlantic.com/business/archive/2013/09/the-law-that-gave-us-the-modern-internet-and-the-campaign-to-kill-it/279588/ [https://perma.cc/3RTP-XGLP].

74. Jones v. Dirty World Entm't Recordings LLC, 755 F.3d 398, 406 (6th Cir. 2014); Klayman v. Zuckerberg, 753 F.3d 1354, 1358 (D.C. Cir. 2014); Doe v. MySpace, Inc., 528 F.3d 413, 422 (5th Cir. 2008); Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1120–21 (9th Cir. 2007); Universal Commc'ns Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 418–19 (1st Cir.

If a broad reading of the safe harbor embodied sound policy in the past, it does not in the present—an era in which child (and adult) predation on the internet is rampant, cybermobs terrorize people for speaking their minds, and designated foreign terrorist groups use online services to organize and promote violent activities. Unless the Court upends the table, it is hard to imagine a retreat from the broad-sweeping interpretation of § 230 adopted in the state and lower federal courts.

B. Radical Changes in the Digital Marketplace

The world of technology companies that § 230 protects today, and the activities of those companies that it immunizes from liability, is immensely different from twenty years ago. At the most basic level, the companies and their successors are vastly larger, more powerful, and less vulnerable than were the nascent "online service providers" of two decades ago. They are also providing services very different—and less obviously about speech—than the Prodigy-like services that Congress sought to protect.

Prodigy was, after all, a bulletin-board system. The major online platforms of the day mostly involved people posting things and expressing opinions about things. The platforms could, to some degree, claim that they were passive actors with regard to the speech of third-party users. That is still true to a point. Social media providers like Twitter and Facebook host the speech of third-party users. Even Omegle is, after all, a facilitator of other people's interactions. It creates chat rooms in which anyone can talk about anything. It is not forcing anyone to talk to children about inappropriate sexual matters.

But the networked environment today is profoundly different from the one in 1996. Twenty years ago, commercial service providers had twelve million subscribers.[75] Now billions of individuals are online in ways that would have been unimaginable when Congress passed the CDA. As Judge Alex Kozinski noted in *Fair Housing Council v. Roommate.com*,[76] "the Internet has outgrown its swaddling clothes and no longer needs to be so gently coddled."[77]

In 1996, it was impossible to foresee the threat to speech imposed by cybermobs and individual harassers, whose abuse chills the speech of those unwilling to subject themselves to further damage.[78] Then, the aggregative power of the internet was not yet known.[79] Today, huge social networks and search engines enable the rapid spread of destructive abuse. If someone posts something defamatory, privacy invasive, or threatening about another person, or even about a nonuser of a given service, and thousands or tens of thousands

2007); Doe v. GTE Corp., 347 F.3d 655, 661–62 (7th Cir. 2003); Green v. Am. Online (AOL), 318 F.3d 465, 471–73 (3d Cir. 2003); Ben Ezra, Weinstein, & Co. v. Am. Online Inc., 206 F.3d 980, 984 (10th Cir. 2000); Zeran v. Am. Online, Inc., 129 F.3d 327, 331–32 (4th Cir. 1997).

75. Reno v. ACLU, 521 U.S. 844, 850–51 (1997).

76. 521 F.3d 1157 (9th Cir. 2008).

77. *Id.* at 1175 n.39.

78. *See* Citron, *supra* note 20, at 119.

79. *Id.*

of people share it, there can be devastating consequences whether or not the targeted individual used the service in question.[80] Online abuse is often the first thing that employers, clients, and potential dates see in a search of a victim's name. The potential for destruction is exponentially greater today than it was twenty years ago.

Moreover, § 230 immunity has been invoked by giant companies engaged in enterprises that have little to do with free expression. This is true for Airbnb, which facilitates short-term rentals of real estate,[81] and eBay, which runs an auction site.[82] It is not hard to imagine § 230's immunity being asserted by Uber, which arranges transportation;[83] Soothe, an on-demand massage service;[84] or Glamsquad, which sends hair stylists to people's homes.[85] These businesses have little to do with free expression, though we have seen business in the on-demand economy asserting § 230's protection with some success.[86] If those companies operated in physical space, they could not escape liability for failing to meet reasonable duties of care.[87]

No doubt, providing a safe harbor for massive social networks, search engines, and internet service providers has been beneficial. If ISPs and other "communication conduits" were not protected by § 230 immunity, they would likely remove valuable online content at the request of hecklers to avoid distributor liability.[88] "The same is true of search engines that index the vast universe of online content and produce relevant information to users

80. CITRON, *supra* note 22, at 5–12.

81. AIRBNB, https://www.airbnb.com/about/about-us [https://perma.cc/L7HA-7KPM] (last visited Oct. 16, 2017).

82. Hinton v. Amazon.com.dedc, 72 F. Supp. 3d 685, 687 (S.D. Miss. 2014) (dismissing the § 230 claim because "claims against eBay arise or 'stem[] from the [] publication of information [on www.ebay.com] created by third parties'" (alterations in original) (quoting Doe v. Myspace, Inc., 528 F.3d 413, 418 (5th Cir. 2008))).

83. *See* Ryan Calo & Alex Rosenblat, *The Taking Economy: Uber, Information, and Power*, 117 COLUM. L. REV. (forthcoming 2017).

84. SOOTHE, https://www.soothe.com/about [https://perma.cc/W2DG-VYPM] (last visited Oct. 16, 2017).

85. Rebecca Adams, *Need a Blowout at Home Within the Hour?: There's an App for That, and It's Called Glamsquad*, HUFFINGTON POST (Mar. 11, 2014), http://www.huffingtonpost.com/2014/03/11/glamsquad_n_4919678.html [https://perma.cc/YP8Y-7MS9].

86. *Compare* Inman v. Technicolor USA, Inc., No. 11-666, 2011 WL 5829024, at *7 (W.D. Pa. Nov. 18, 2011) (finding eBay immune from liability for mercury poisoning contracted by the plaintiff after purchasing vacuum tubes from a third party on the site), *with* Airbnb, Inc. v. San Francisco, 217 F. Supp. 3d 1066, 1072–73 (N.D. Cal. 2016) (finding § 230 immunity inapplicable because a city ordinance "does not regulate what can or cannot be said or posted in the listings" and "creates no obligation . . . to monitor, edit, withdraw or block the content supplied by hosts" but rather holds Airbnb liable "only for [its] own conduct").

87. Landlords, shopping malls, hospitals, and banks have been held liable for enabling foreseeable criminal activity of third parties. *See* Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1582 (2005); *see also* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1836–38 (2010) (arguing that privacy invasions should be addressed by mainstream torts like negligent enablement, but § 230's broad immunity has often stood in the way); Robert L. Rabin, *Enabling Torts*, 49 DEPAUL L. REV. 435, 443 n.41 (1999) (arguing that there is little difference between inciting misconduct and enabling it).

88. CITRON, *supra* note 22, at 171.

in seconds and, for that matter, social media providers that host millions, even billions, of users."[89]

We recognize how § 230 of the CDA has benefitted digital expression specifically and democracy generally. We are not arguing that § 230 should not exist or that it should not offer robust protections for platform providers. Instead, we want to bring its expressive and other costs into view along with its benefits so that courts can recalibrate the interpretative lens of the CDA's safe harbor.

Although § 230 has secured breathing space for the development of online services and countless opportunities to work, speak, and engage with others, it has also produced unjust results. An overbroad reading of the CDA has given 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.[90] Companies have too limited an incentive to insist on lawful conduct on their services beyond the narrow scope of their terms of service. They have no duty of care to respond to users or larger societal goals. They have no accountability for destructive uses of their services, even when they encourage those uses. In addition, platforms have invoked § 230 in an effort to immunize many activities that have very little to do with speech.[91]

The permissive interpretation of § 230's immunity eliminates "incentives for better behavior by those in the best position to minimize harm."[92] As Citizen Media Law Project's Sam Bayard has explained, a site operator can enjoy § 230 immunity all the while "building a whole business around people saying nasty things about others, and . . . affirmatively choosing not to track user information that would make it possible for an injured person to go after the person directly responsible."[93]

Let's take stock of some providers and users whose activities have been immunized or seem likely to enjoy immunity from liability under the broad approach to § 230:

- a revenge porn operator whose business was devoted to posting people's nude images without consent[94]
- a gossip site that urged users to send in "dirt" and fanned the flames with snarky comments[95]

---

89. *Id.*

90. *Id.*; *see also supra* notes 57–60 and accompanying text.

91. Hinton v. Amazon.com.dedc, 72 F. Supp. 3d 685, 687 (S.D. Miss. 2014).

92. Citron, *supra* note 20, at 118; Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. ON TELECOMM. & HIGH TECH. L. 101, 105, 119 (2007).

93. Sam Bayard, *New Jersey Prosecutors Set Sights on JuicyCampus*, DIGITAL MEDIA L. PROJECT (Mar. 21, 2008, 12:41 PM), http://www.dmlp.org/blog/2008/new-jersey-prosecutors-set-sights-juicycampus [https://perma.cc/PK6J-ZZ6D].

94. CITRON, *supra* note 22, at 168–81. As the advocacy group Cyber Civil Rights Initiative (run by Dr. Holly Jacobs and Professor Mary Anne Franks) has shown, there are countless sites whose raison d'être is the peddling of nonconsensual pornography.

95. Jones v. Dirty World Entm't Recordings LLC, 755 F.3d 398, 402–03 (6th Cir. 2014); *see also* Eric Goldman, *Want to Encourage Gossipy Content Online?: Go for It—Sarah Jones vs. TheDirty*, FORBES (June 11, 2014, 9:49 PM), https://www.forbes.com/sites/ericgoldman/

- a message board that knew about users' illegal activity yet refused to collect information that would allow them to be held accountable[96]
- a purveyor of sex-trade advertisements whose policies and architecture were designed to prevent the detection of sex trafficking[97]
- an auction site facilitating the sale of goods that risked serious harm[98]
- an individual who forwarded a defamatory email with a comment that "[e]verything will come out to the daylight"[99]
- a hook-up site that ignored more than fifty reports that one of its subscribers was impersonating a man and falsely suggesting his interest in rape, resulting in hundreds of strangers confronting the man for sex at work and home[100]

Blanket immunity gives platforms a license to solicit illegal activity, including sex trafficking, child sexual exploitation, and nonconsensual pornography.[101] Site operators have no reason to take down material that is clearly defamatory or invasive of privacy.[102] They have no incentive to respond to clear instances of criminality or tortious behavior. Victims have no leverage to insist that operators take down destructive posts.

III. MODEST SOLUTIONS

It is not inevitable that society must suffer these harmful consequences in exchange for a legal environment that fosters speech and innovation. It's a choice—and it's a bad choice. Ideally, since § 230 does not actually compel

2014/06/17/want-to-encourage-gossipy-content-online-go-for-it [https://perma.cc/YX3X-FF3R].

96. Citron, *supra* note 20, at 118 n.388; Bayard, *supra* note 93 (arguing that § 230 should not, but nonetheless does, immunize from liability sites like AutoAdmit and JuicyCampus that solicited defamation and told users that it would do what they could to prevent them from being traced and held accountable).

97. Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 16 (1st Cir. 2016), *cert. denied*, 137 S. Ct. 622 (2017) (No. 16-276).

98. Inman v. Technicolor USA, Inc., No. 11-666, 2011 WL 5829024, at *7 (W.D. Pa. Nov. 18, 2011).

99. Phan v. Pham, 105 Cal. Rptr. 3d 791, 795 (Ct. App. 2010).

100. Herrick v. Grindr, No. 17-CV-932 (VEC), 2017 WL 744605, at *1 (S.D.N.Y. Feb. 24, 2017); Andy Greenberg, *Spoofed Grindr Accounts Turned One Man's Life into a Living Hell*, WIRED (Jan. 31, 2017), https://www.wired.com/2017/01/grinder-lawsuit-spoofed-accounts/ [https://perma.cc/WP6D-M344]; Sarah Ashley O'Brien, *1,100 Strangers Showed Up at His Home for Sex. He Blames Grindr*, CNN (Apr. 14, 2017), http://www.money.cnn.com/2017/04/14/technology/grindr-lawsuit/index.html [https://perma.cc/GT9S-3G8R].

101. DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 159 (2007).

102. Indeed, the broad reading of § 230 is why revenge porn operators have been so brazen about their business model. CITRON, *supra* note 22, at 173–76. Some operators have learned the hard way that § 230 does not protect them from liability related to their *own* wrongdoing. *Id.* Kevin Bollaert was convicted of engaging in an extortion scheme in California after he charged "up to $350" a photo for the removal of nonconsensual pornography. *Id.* Hunter Moore pleaded guilty to federal conspiracy to hack women's computers to steal intimate images. *See* Nicky Wolf, *"Revenge Porn King" Hunter Moore Pleads Guilty to Hacking Charges*, GUARDIAN (Feb. 19, 2015, 10:59 AM) https://www.theguardian.com/technology/2015/feb/19/revenge-porn-hunter-moore-pleads-guilty-hacking-identify [https://perma.cc/TQ4X-9HRN].

this result, the solution would be for courts to interpret § 230 in a manner more consistent with its text, context, and history. That would go a long way to incentivize efforts to deter illegal material, which is what the CDA's drafters set out to do in the first place. This is probably a long shot given the judiciary's current understanding of the law. If so, the only course is a potential statutory fix. We suggest a course correction for the courts and, if needed, a modest statutory change that would help reorient the current liability environment.

A. Interpretative Shift

As a preliminary matter, courts should not apply § 230's safe harbor unless the claims relate to the publication of user-generated content. Some recent decisions have embraced this approach. In *Doe v. Internet Brands, Inc.*,[103] two men used a networking site devoted to the modeling industry to lure the plaintiff to an audition where they drugged her, raped her, and recorded the rape.[104] The woman sued the site's owner because it knew about the rapists' use of the site but never issued a warning about it.[105] The Ninth Circuit rejected the § 230 defense because the defendant was not being sued for publishing third-party content.[106] Because the lawsuit centered on defendant's failure to warn the plaintiff about the rape scheme rather than for its failure to edit or remove content, the court rejected the defendant's invocation of § 230.[107]

This reading of the statute is consistent with the fact that "publisher" and "speaker" are terms of art in defamation and intellectual property law.[108] The *Prodigy* decision, which prompted lawmakers to adopt the safe harbor, involved defamation law.[109] Had Congress intended to extend a broad cloak of immunity to providers beyond decisions related to the publication of content, one would expect it to have said so. Congress did not even prohibit holding providers liable for the dissemination of information; it merely prohibited a finding that a provider was a "publisher" or "speaker."[110] Courts should, at a minimum, limit the statute to those terms.

This reading would set a limit on the kinds of claims covered by § 230. Many legal theories advanced under the law do not turn on whether a defendant is a "publisher" or "speaker."[111] Liability for aiding and abetting

103. 824 F.3d 846 (9th Cir. 2016).
104. *Id.* at 851.
105. *Id.* at 852.
106. *Id.*
107. *Id.* at 851.
108. RESTATEMENT (SECOND) OF TORTS § 581 (AM. LAW INST. 1977); Pamela Samuelson & Robert J. Glushko, *Intellectual Property Rights for Digital Library and Hypertext Publishing Systems*, 6 HARV. J.L. & TECH. 237, 237 n.3 (1993).
109. Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *3 (N.Y. Sup. Ct. May 24, 1995).
110. 47 U.S.C. § 230(c)(1) (2012).
111. That is certainly true of tort claims like intentional infliction of emotional distress, criminal penalties for video voyeurism, and civil rights law. CITRON, *supra* note 22, at 121–26.

others' wrongful acts does not depend on the manner in which aid was provided.[112] Designing a site to enable defamation or sex trafficking could result in liability in the absence of a finding that a site was being sued for publishing or speaking.

In addition to a narrow reading of "publisher" and "speaker" under § 230(c)(1), courts should limit its application to Good Samaritans.[113] Section 230's title reflects this purpose: "[p]rotection for private blocking and screening of offensive material."[114] So does subsection (c)'s subtitle: "[p]rotection for 'Good Samaritan' blocking and screening of offensive material."[115] "[T]he title of a statute and the heading of a section are 'tools available for the resolution of a doubt' about the meaning of a statute."[116]

Sites like The Dirty[117] and Backpage[118] have successfully argued that § 230(c)(1) provides them with blanket immunity related to user-generated content. They read a provision enacted to encourage providers to restrict abusive material to shield them from liability for encouraging the posting of such material.[119] This interpretation undermines the congressional goal of incentivizing self-regulation.[120]

The courts should certainly not extend the CDA's safe harbor to Bad Samaritans. Instead, § 230(c)(1) should be read to apply only to Good Samaritans envisioned by its drafters: providers or users engaged in good faith efforts to restrict illegal activity, as was true of Prodigy. None of the CDA's congressional purposes apply where platforms benefit from material's destructive nature. Extending immunity to Bad Samaritans undermines § 230's mission by eliminating incentives for better behavior by those in the best position to minimize harm. Treating abusive website operators and Good Samaritans alike devalues the efforts of the latter and may result in less of the very kind of blocking that the CDA in general, and § 230 in particular, sought to promote.[121]

What activity would warrant treating a provider as a Good Samaritan under § 230(c)(1)? Grants of immunity typically seek to protect and encourage specific beneficial acts. That is why law often immunizes Good Samaritans

---

112. *Id.* at 125.

113. Citron, *supra* note 20, at 116 n.377.

114. 47 U.S.C. § 230.

115. *Id.* § 230(c).

116. Almendarez-Torres v. United States, 523 U.S. 224, 234 (1998) (quoting Bhd. of R.R. Trainmen v. Balt. & Ohio R.R., 331 U.S. 519, 528–29 (1947)); *see also* Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 670 (7th Cir. 2008) ("Why not read § 230(c)(1) as a definitional clause rather than as an immunity from liability, and thus harmonize the text with the caption?").

117. Jones v. Dirty World Entm't Recordings LLC, 755 F.3d 398, 402–03 (6th Cir. 2014).

118. Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 16 (1st Cir. 2016), *cert. denied*, 137 S. Ct. 622 (2017) (No. 16-276).

119. *See supra* notes 117–17 and accompanying text.

120. Section 230(e)(3) disclaims any intent "to prevent any State from enforcing any State law that is consistent with this section" but bars any "that is inconsistent with this section." 47 U.S.C. § 230(e)(3). Ascertaining § 230's effect on operators' liability for state law requires an analysis of its purpose.

121. Citron, *supra* note 20, at 116.

for negligence but not for intentional torts or crimes.[122] For instance, under state law, physicians may enjoy immunity from liability for volunteering to treat a stricken stranger.[123] Protection from liability does not extend to the Good Samaritan's practicing of medicine without a license or intentionally harming the sick stranger.[124] If providers or users engage in good-faith efforts to address or restrict abusive material, they should be immune from liability even if they were negligent or reckless in doing so.[125] By contrast, the immunity should not apply to platforms designed to host illegality or sites that deliberately choose to host illegal content.

What about The Dirty? The site should not be protected from liability since it is designed for the express purpose of hosting defamation and privacy invasions. To immunize it would turn the notion of the Good Samaritan on its head since its interests are aligned with the abusers. Enjoying § 230 would be a windfall for the site operator who gives lip service to preventing defamation in the site's terms of service but encourages his "Dirty Army" to email him "dirt" and then chooses gossip to post.[126]

Now back to Omegle. If the site were designed to facilitate the sexual exploitation of children, then it should certainly not be immunized from liability. But let's suppose this is not the case; after all, the site does say it is monitoring video chats and warns users that sexual predators have been

122. *See, e.g.*, Mitchell v. Forsyth, 472 U.S. 511, 536 (1985) (providing no prosecutorial immunity for the attorney general's authorization of wiretaps for purported national security purposes).

123. *See, e.g.*, CAL. HEALTH & SAFETY CODE § 1799.102 (West 2009) (protecting medical personnel "who in good faith, and not for compensation, renders emergency medical or nonmedical care" in an emergency); CONN. GEN. STAT. § 52-557b (2016) (protecting persons "licensed to practice medicine and surgery" in Connecticut and "any other state of the United States" from liability for providing "emergency medical or professional assistance"); MD. CODE ANN., CTS. & JUD. PROC. § 5-603 (West 2016) (protecting persons "licensed by [Maryland] to provide medical care" from civil liability "for any act or omission in giving any assistance or medical care" in an emergency situation). *See generally* Patricia H. Stewart, William S. Agin & Sharon P. Douglas, *What Does the Law Say to Good Samaritans?: A Review of Good Samaritan Statutes in 50 States and on U.S. Airlines*, 143 CHEST 1774 (2013) (providing an overview of Good Samaritan state statutes in the United States as well as the federal Aviation Medical Assistance Act, which protects physicians providing emergency assistance on aircraft registered in the United States).

124. *See, e.g.*, MD. CODE ANN., CTS. & JUD. PROC. § 5-603 (stating that a person not licensed to provide medical care may provide emergency medical assistance but must "relinquish[] care of the victim when someone who is licensed or certified . . . to provide medical care or services becomes available"); N.C. GEN. STAT. § 90-21.14 (2014) (protecting persons who "render[] first aid or emergency health care treatment" from liability due to injuries or death "unless it is established that the injuries were or the death was caused by gross negligence, wanton conduct or intentional wrongdoing" by the person providing emergency care); S.C. CODE ANN. § 15-1-310 (2017) (stating that "any person" who provides emergency assistance is not liable "for any personal injury as a result of any act or omission . . . except acts or omissions amounting to gross negligence or willful or wanton misconduct").

125. Olivier Sylvain has a thoughtful proposal to revise the Good Samaritan obligation in § 230 to shift away from good-faith efforts at self-regulation. Olivier Sylvain, *Intermediary Design Duties*, 50 CONN. L. REV. (forthcoming 2017). Instead, Professor Sylvain would bar the immunity when providers process and publish user data in ancillary or secondary markets in ways that their originating users did not intend. *Id.*

126. Knibbs, *supra* note 8.

known to use its services.[127] Imagine that the site is given credible information about a specific sexual predator using its services and decides to do nothing about it. The family of a child exploited by that predator should be able to sue the site for knowingly enabling criminal activity. If the site knows predators are using its services and takes no meaningful action to stop them, it should not be categorically immune from suit related to the decision to make its service available to predators. There is no particular reason, even under current law, to treat the decision to give predators access to children as the act of a "publisher" or "speaker." And it certainly is not the act of a Good Samaritan.

By contrast, Twitter likely would enjoy immunity from liability for the delayed removal of ISIS accounts. Depending on the circumstance, the failure to remove specific ISIL accounts might be understood as negligent or reckless conduct falling within the safe-harbor immunity. Given the scale of Twitter's user base (in the hundreds of millions), Twitter should be immunized from liability for failing to remove designated foreign terrorist group accounts of which it had no notice or to which it did not have reasonable time to react. The platform is currently engaged in good-faith efforts to screen and respond to complaints that accounts are being run by designated foreign terrorist groups. In the first six months of 2017, the platform removed close to 377,000 proterrorism accounts.[128] Sustained failure to remove an ISIS account despite repeated notifications, by contrast, might well strip the company of immunity in a specific case. Note that this would not in and of itself give rise to liability. Instead, it would merely require that Twitter defend a suit on its merits rather than being automatically shielded from answering claims asserted against it.

B. Legislative Proposal

If the courts decline to move § 230 in this direction, Congress should consider statutory changes. There have been several suggestions for fixing § 230. The National Association of Attorneys General (NAAG) has urged Congress to amend § 230 to exempt state criminal laws.[129] This proposal grew out of concerns about advertisements for child-sex traffickers.[130] But

127. *See supra* notes 3–5 and accompanying text.

128. Liat Clark, *Twitter's Spam Tools Helped Shut Down 376,890 Terrorist Accounts in 6 Months*, WIRED (Mar. 21, 2017), http://www.wired.co.uk/article/twitter-transparency-report-2017 [https://perma.cc/2GV3-YLH2]. Going forward the problem for the major social media sites like Twitter may not be removing too little extremist speech but rather removing too much in the face of threatened regulation by the European Union and its member states. *See* Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. (forthcoming 2018). EU member countries have effectively compelled the major tech companies to adopt their speech norms with threats of onerous new laws and penalties, which poses serious risk of censorship creep. *Id.*

129. Mike Masnick, *More Details Emerge as States' Attorneys General Seek to Hold Back Innovation on the Internet*, TECHDIRT: INNOVATION (June 19, 2013), https://www.techdirt.com/blog/innovation/articles/20130619/01031623524/more-details-emerge-as-states-attorneys-general-seek-to-hold-back-innovation-internet.shtml [https://perma.cc/6ZTF-SRBG].

130. CITRON, *supra* note 22, at 177.

the NAAG proposal would require online providers to shoulder burdensome legal compliance with countless state criminal laws that have nothing to do with the most troubling uses of online platforms, such as child-sex trafficking, stalking, and nonconsensual pornography.

A modest alternative to a sweeping elimination of the immunity for state law would be to eliminate the immunity for the worst actors. As one of us (Citron) has proposed, sites that encourage destructive online abuse or that know they are principally used for that purpose should not enjoy immunity from liability.[131] Mirroring § 230's current exemption of federal law and intellectual property, the amendment could state:

> "Nothing in Section 230 shall be construed to limit or expand the application of civil or criminal liability for any website or other content host that purposefully encourages cyber stalking[,] . . . nonconsensual pornography,"[132] sex trafficking, child sexual exploitation, or that has knowledge that it principally hosts such material.

A broader though still balanced approach would be to clarify the reach of § 230(c)(1), which could be revised as follows:

> No provider or user of an interactive computer service that *takes reasonable steps to prevent or address unlawful uses of its services* shall be treated as the publisher or speaker of any information provided by another information content provider *in any action arising out of the publication of content provided by that information content provider*.

With this revision, platforms would enjoy immunity from liability if they could show that their response to unlawful uses of their services was reasonable. Such a determination would take into account differences among online entities. ISPs and social networks with millions of postings a day cannot plausibly respond to complaints of abuse immediately, let alone within a day or two. To return to some examples, Twitter would be in a strong position to argue that it has taken reasonable steps to address ISIS and other designated foreign terrorist groups on its platform—thus it would likely enjoy immunity for such postings. Omegle, we suspect, could make no such showing—it would likely not be immune under such a standard. Sites that encourage the posting of nonconsensual pornography and ignore victims' requests to remove their nude images would not be understood as acting reasonably to address illegality.

C. The Sky Will Not Fall

Our proposal will face opposition on two major grounds. The first involves free speech and the second concerns innovation. In this Part, we respond to both concerns.

Broad-sweeping immunity for online platforms is not required by the First Amendment. Section 230 involves a policy layer on top of the First

131. *Id.*

132. *Id.* (noting that, "[i]n amending section 230, Congress could import the definition of cyberstalking" from the federal interstate stalking statute, 18 U.S.C. § 2261A (2012)).

Amendment, and we are proposing a decidedly modest shift in it. Our proposal would not eliminate § 230's safe harbor. Instead, the safe harbor would be limited to providers or users that have taken reasonable steps to prevent or address the illegality of which plaintiffs are complaining.

Our proposal leaves dramatically more protection in place than is currently accorded the physical operations of newspapers or colleges. The *Washington Post*, for instance, does not enjoy blanket immunity from having to defend a lawsuit for publishing an article. Color us skeptical that online providers really need dramatically more protection than do newspapers to protect free expression in the digital age—and particularly, that they need that protection for all sorts of actions that have nothing to do with speech. In the world we envision, the CDA's immunity provision would be unavailable to operators only when they cannot make a cogent argument that they are behaving reasonably to stop illegal activity. The consequence of that failure, in our scheme, is not even liability; it is merely the removal of an absolute shield from the possibility of liability.

We are skeptical that § 230, as currently interpreted, is really optimizing free speech. It gives an irrational degree of free speech benefit to harassers and scofflaws but ignores important free speech costs to victims. Individuals have difficulty expressing themselves in the face of online assaults.[133] They shut down their blogs, sites, and social network profiles not because they tire of them but because continuing them provokes their attackers.[134] Civil liberties organization Electronic Frontier Foundation has recognized that cyberharassment is "profoundly damaging to the free speech and privacy rights of the people targeted."[135] Neil Richards and one of us (Citron) have argued that a robust culture of free speech online can be achieved without shielding from liability those who deliberately repost illegal material or those who run sites whose business model is hosting such abuse.[136] An environment of perfect impunity for intermediaries that facilitate online abuse is not an obvious win for free speech if the result is that the harassers speak unhindered and the harassed retreat in fear offline.

A recalibrated § 230 would, we think, do a better job of incentivizing the best-positioned parties to protect against risks to free expression engendered

133. Danielle Keats Citron, *Online Engagement on Equal Terms*, B.U. L. REV. ONLINE (Oct. 19, 2015), https://www.bu.edu/bulawreview/citron-online-engagement-on-equal-terms/ [https://perma.cc/C5DT-N5KD].

134. Citron, *supra* note 20, at 116 (arguing that combating cyberharassment with a cyber-civil rights legal agenda would help preserve online dialogue and promote a culture of political, social, and economic equality).

135. Danny O'Brien & Dia Kayyali, *Facing the Challenge of Online Harassment*, ELECTRONIC FRONTIER FOUND. (Jan. 8 2015), https://www.eff.org/deeplinks/2015/01/facing-challenge-online-harassment [https://perma.cc/BJS3-XTDH] (noting that cyber harassment silences people, especially those with "less political or social power" and "women and racial and religious minorities").

136. Danielle Keats Citron & Neil Richards, *Can and Should Perez Hilton Be Held Liable for Reposting of Celebrities' Nude Photos Without Their Consent?*, FORBES (Sept. 3, 2014), https://www.forbes.com/sites/daniellecitron/2014/09/03/can-and-should-perez-hilton-be-held-liable-for-reposting-celebrities-private-nude-photos-without-their-consent/ [https://perma.cc/PD2N-X4LB].

by online abuse. By contrast, the current approach allows providers to host abuse without regard for the harm it inflicts. As one of us (Wittes) has argued with Gabriella Blum in a different context, the internet "lacks any kind of sensible allocation of risk."[137] ISPs and software vendors suffer no real consequences for bad cybersecurity; thus, bad security and low quality are the norm.[138] If § 230 is left as is, the same will continue to be true of online platforms and the illegal behavior they host. Of course, websites whose business model is abuse have no incentive to restrict it. But neither do sites that know about unlawful activity and turn a blind eye in case it might appeal to some users.

What is more, to the extent our proposal is resisted on the grounds that online platforms deserve special protection from liability because they operate as zones of public discourse, we offer the modest rejoinder that while the internet is special, it is not so fundamentally special that all normal legal rules should not apply to it. Yes, online platforms facilitate expression, along with other key life opportunities, but no more and no less so than do workplaces, schools, and coffee shops, which are all also zones of conversations and are not categorically exempted from legal responsibility for operating safely. The law has not destroyed expression in workplaces, homes, and other social venues. When courts began recognizing claims under Title VII for sexually hostile work environments, employers argued that the cost of liability would force them to shutter, and if not, would ruin the camaraderie of workspaces.[139] As we know now, that has not been the case. Rather, those spaces are now available to all on equal terms while firms have more than survived in the face of Title VII liability. The same should be true for networked spaces.

This argument is part of a much broader argument that a strong liability shield is necessary to help the internet flourish. Such a shield made a certain amount of sense in the early years of the internet, when it was unclear how robustly the internet would develop. It makes little sense now. As the Ninth Circuit has underscored:

> The Internet is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of laws and regulations applicable to brick-and-mortar businesses. Rather, it has become a dominant—perhaps the 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 the immunity provided by Congress and thus give online businesses an unfair advantage over their real-world counterparts, which must comply with laws of general applicability.[140]

---

137. BENJAMIN WITTES & GABRIELLA BLUM, THE FUTURE OF VIOLENCE: ROBOTS AND GERMS, HACKERS AND DRONES 216 (2015).

138. *Id.* at 217.

139. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 107 (2000). Serious thanks to Mary Anne Franks for our discussions about these and so many other related issues.

140. Fair Hous. Council v. Roommate.com, LLC, 521 F.3d 1157, 1164 n.15 (9th Cir. 2008).

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.[141] As the industry matured, the liability protection weakened, and cars became "dramatically safer."[142]

This is part of a notable pattern. Technological advances tend to create large, successful business entities. Those injured by new technologies see those businesses as fitting sources of compensation. The building of canals, railroads, and reservoirs at the dawn of the Industrial Revolution contributed much to the economy, yet they also inflicted destruction on adjoining property owners and towns, much of it wholly unnecessary.[143]

"The law's reaction to claims against such large actors for new types of harms typically goes through" distinct phases.[144] Law first recognizes the new form of harm but not the benefit that the new technology has occasioned.[145] 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.[146] Once the technology becomes better established, law recognizes that not all liability awards threaten its survival.[147] Law then separates activities that are indispensable to the pursuit of the new industry from behavior that causes unnecessary harm to third parties.[148] This is what the celebrated *Palsgraf v. Long Island Railroad Co.*[149] 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.

We want to suggest that, with respect to content intermediaries, we are currently in the midst of this pattern. The first hypervigilant stage can be seen in a few early cases, notably *Prodigy*, in which courts found online service providers liable for offensive material that came through their portals.[150] Ironically, Prodigy's liability was based in part on its having

141. WITTES & BLUM, *supra* note 137, at 216.
142. *Id.*
143. MORTON J. HORWITZ, THE TRANSFORMATION OF AMERICAN LAW, 1780–1860, at 71 (1977).
144. Citron, *supra* note 20, at 115.
145. HORWITZ, *supra* note 143, at 71–74.
146. Citron, *supra* note 20, at 115.
147. *Id.*
148. Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 276–77 (2007).
149. 162 N.E. 99 (N.Y. 1928).
150. Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *4 (N.Y. Sup. Ct. May 24, 1995) (finding that Prodigy—in control of the content on its platform—is a publisher and thus liable for offensive content that is posted).

attempted to screen out troubling material.[151] That its good-faith remedial measures were used to establish liability moved Congress to immunize such actions in the CDA's section 230. The CDA "checked a particular excess of law's hyper-vigilant stage."[152] The law reached the next hyperprotective stage as courts "read section 230 to grant sweeping immunity far beyond what its words and context supported."[153] These efforts have prevented the courts from exploring what standard of care ought to apply to ISPs and website operators.[154]

As we have noted elsewhere, the ideal solution would be to move the law to the third, more analytic stage.[155] "It opposes holding ISPs liable merely because of their deep pockets and inevitable proximity to harm. It thus is sympathetic to the results, if not the reasoning, of many of the cases rejecting liability."[156] This solution opposes "blanket grants of immunity" that leave innocent victims of cyber mobs, sex traffickers, terrorist violence, and other forms of abuse without effective recourse even where they can show that intermediaries encouraged the bad actors who injured them.[157]

Instead, our proposal seeks to establish a reasonable standard of care that will reduce opportunities for abuses without interfering with the further development of a vibrant internet or unintentionally turning innocent platforms into involuntary insurers for those injured through their sites.[158] Approaching the problem as one of setting an appropriate standard of care would more readily allow for differentiation between various online actors; this approach would provide different rules for websites established to facilitate mob attacks vis-à-vis large ISPs linking millions to the internet. Courts must abandon their hyperprotective posture to bring about this positive change.[159]

CONCLUSION

An immunity provision designed to encourage voluntary blocking and removal of illegal material should not shield providers that encourage or deliberately host such material. An overbroad reading of the CDA has given platforms a free pass to ignore destructive activities and, worse, to solicit unlawful activities while doing what they can to ensure that abusers cannot be identified. With modest adjustments to § 230, either through judicial interpretation or legislation, we can have a robust culture of free speech online without extending the safe harbor to Bad Samaritans.

---

151. *Id.* (finding it notable that Prodigy "held itself out to the public and its members as controlling the content of its computer bulletin boards"); Citron, *supra* note 20, at 115.
152. Citron, *supra* note 20, at 116.
153. *Id.*
154. *Id.* at 117.
155. *Id.*
156. *Id.*
157. *Id.*
158. *Id.*
159. *Id.*