BYU Law Review

Volume 47 | Issue 5 Article 6

Summer 6-20-2022

The Internet Immunity Escape Hatch

Gregory M. Dickinson

The Internet Immunity Escape Hatch

Gregory M. Dickinson[*]

Internet immunity doctrine is broken, and Congress is helpless. Under Section 230 of the Communications Decency Act of 1996, online entities are absolutely immune from lawsuits related to content authored by third parties. The law has been essential to the internet's development over the last twenty years, but it has not kept pace with the times and is now deeply flawed. Democrats demand accountability for online misinformation. Republicans decry politically motivated censorship. And all have come together to criticize Section 230's protection of bad-actor websites. The law's defects have put it at the center of public debate, with more than two dozen bills introduced in Congress in the last year alone.

Despite widespread agreement on basic principles, however, legislative action is unlikely. Congress is deadlocked, unable to overcome political polarization and keep pace with technological change. Rather than add to the sizeable literature proposing changes to the law, this Article asks a different question—how to achieve meaningful reform despite a decades-old statute and a Congress unable to act. Even without fresh legislation, reform is possible via an unlikely source: the Section 230 internet immunity statute that is already on the books. Because of its extreme breadth, Section 230 grants significant interpretive authority to the state and federal courts charged with applying the statute. This Article

* Assistant Professor of Law and, by courtesy, Computer Science, St. Thomas University College of Law; Nonresidential Fellow, Stanford Law School Program in Law, Science & Technology; J.D., Harvard Law School. For their insights and generous comments, thanks to Sam Bray, Zach Catanzaro, Thomas Kadri, Dmitry Karshtedt, Kate Klonick, Mark Lemley, Irina Manta, Riana Pfefferkorn, Alan Rozenshtein, Ira Nathenson, David Thaw, Claire Wright, and participants at the Nebraska Governance and Technology Center Law & Technology Workshop in July 2021, the Central States Law Schools Association Annual Scholarship Conference in September 2021, and the Yale Law School Information Society Project Technologies of Deception Conference in March 2022. Karla Alberte Gonzalez and Genesis M. Perez provided excellent research assistance and valuable suggestions.

shows how, without any change to the statute, courts could press forward with the very reforms on which Congress has been unable to act.

CONTENTS

INTRODUCTION

Congress is drowning in internet reform proposals. The technologies that have transformed nearly every facet of human activity—from how we work, shop, and eat, to how we debate politics and connect with family and friends—are now dominated by a few of the nation's biggest tech companies, which hold the power to track our movements, influence purchasing decisions, regulate the flow of information, and shape political discourse. With this great power has come great controversy. Lawmakers from both parties are alarmed by tech companies' unchecked power. As private companies, they make their decisions behind closed doors, free from public scrutiny, and yet, as online rather than physical-world entities, they enjoy immunity from many of the rules that govern their analog counterparts.

At the heart of the controversy lies Section 230[1] of the Communications Decency Act of 1996,[2] a statute whose importance to the modern internet is difficult to overstate. Since its enactment more than twenty years ago, Section 230 has been a resounding success.[3] Its broad protections against lawsuits related to third-party content shield online entities from an economically crippling duty to review and moderate the deluge of data that flows through their systems.[4] Without such protection, online platforms might be compelled to censor user speech or disallow online posting altogether to avoid the risk of liability.[5] Section 230's protections have been crucial to the free speech advances of the last two decades.

But Section 230—as interpreted by the courts—has not kept pace with the times and now presides over a very different internet from the one it was designed to govern. A law designed to foster free expression now protects entities even if they choose to silence disfavored viewpoints. And, despite its publication-centric roots, Section 230 now insulates online entities from liability for all manner of lawsuits, including product-defect claims—such as the one brought against Snapchat for the design of the app's speed filter,[6] which resulted in many accidents by teenage drivers—and claims involving intentional wrongdoing, like the sex-trafficking conspiracy claim brought against the website Backpage.com by sex-trafficking victims who alleged the site had hosted "escort" ads depicting themselves and other underage girls and had intentionally obstructed law-enforcement efforts against sex traffickers so that it could continue to profit from the ad sales.[7]

1. 47 U.S.C. § 230.

2. Communications Decency Act of 1996, Pub. L. No. 104-104, tit. V, 110 Stat. 56, 133–43 (codified in 47 U.S.C. §§ 201, 223, 303, 330, 531–32, 551, 559–61; 18 U.S.C. §§ 1465, 2422).

3. *See* JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET 145–63 (2019) (discussing Section 230's impact on the American technology industry in the years following its enactment).

4. *See infra* Section I.A.

5. *Id.*

6. Lemmon v. Snap, Inc., 440 F. Supp. 3d 1103 (C.D. Cal. 2020).

7. Doe v. Backpage.com, LLC, 817 F.3d 12, 16–17, 20–21 (1st Cir. 2016), *cert. denied*, 137 S. Ct. 622 (2017), *superseded by statute*, Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (FOSTA), Pub. L. No. 115-164, 132 Stat. 1253, *as recognized in* Teatotaller, LLC v. Facebook, Inc., 242 A.3d 814, 820 (N.H. 2020).

Every day brings fresh controversy, call for change, or proposed legislation.[8] From cyberbullying,[9] online governance,[10] and freedom of expression,[11] to big-tech antitrust concerns,[12]

8. *See infra* Section III.B (discussing numerous reform bills pending in Congress that would address perceived flaws in the current internet immunity regime, including volitional online wrongdoing, special treatment of online versus offline entities, and platforms' content-moderation practices).

9. *See* Erica Goldberg, *Free Speech Consequentialism*, 116 COLUM. L. REV. 687, 744–45 (2016) (noting that current internet immunity doctrine bars claims against online entities for revenge porn and other forms of cyberbullying); Andrew Gilden, *Cyberbullying and the Innocence Narrative*, 48 HARV. C.R.-C.L. L. REV. 357, 389–90 (2013) (critiquing proposals to narrow online immunity to protect gay teens from harassment on ground that such efforts obscure the power of individual agency).

10. *See* Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1182–93 (2018) (discussing platforms' role as regulators of free speech in digital era); Jennifer Daskal, *Speech Across Borders*, 105 VA. L. REV. 1605, 1637–44 (2019) (discussing geographic scope of online platforms' content-filtering determinations and implications for territorial sovereignty); Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1599–613 (2018) (tracing the ability of private platforms like Facebook to make content-moderation decisions regarding user-submitted content to Section 230); Frank Pasquale, *Two Narratives of Platform Capitalism*, 35 YALE L. & POL'Y REV. 309, 316–19 (2016) (offering two possible narratives of the distributed online platform and implications for each on regulatory and self-governance policy decisions); *see also* David R. Johnson & David Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996) (arguing just after Section 230's enactment that internet regulation would require its own distinct principles); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 502 (1999) (arguing that the study of cyberlaw can illuminate principles that affect the real world).

11. *See* Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035, 1036–40 (2018) (exploring the departure of online platforms from U.S. First Amendment values and the dangers of bowing to international pressure to self-regulate); Danielle Keats Citron & Helen Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*, 91 B.U. L. REV. 1435, 1453–84 (2011) (noting that Section 230 insulates platforms from legal liability and offering proposals for online platforms to voluntarily respond to online hate speech); Eric Goldman, *Why Section 230 Is Better Than the First Amendment*, 95 NOTRE DAME L. REV. REFLECTION 33, 36–46 (2019) (discussing Section 230's enhanced substantive and procedural protections for online entities beyond those of the First Amendment); Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendmen*t, 76 GEO. WASH. L. REV. 986, 1009 (2008) (arguing that Section 230 immunity should include a corresponding limit on an intermediary's ability to censor speech); Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87 NOTRE DAME L. REV. 293, 295–96 (2011) (noting speech-enhancing effects of Section 230 due to its preventing imposition of liability on intermediaries for harmful or offensive speech that those intermediaries might otherwise be pressured to censor).

12. *See* C. Scott Hemphill, *Disruptive Incumbents: Platform Competition in an Age of Machine Learning*, 119 COLUM. L. REV. 1973, 1974–93 (2019) (identifying potential sources of competition among dominant participants in online platform market and offering proposals to maximize competition); Lina M. Khan, *The Separation of Platforms and Commerce*, 119 COLUM. L. REV. 973, 1037–92 (2019) (proposing bars on entities' engaging in new lines of business as a check on dominance of a small number of tech firms); Lina M. Khan & David

privacy,[13] and tort liability,[14] the effects of internet immunity law are as wide ranging as the internet itself.

Section 230 continues to play a critical role governing internet liability, but its defects have put it at the center of public debate. Reform proposals abound; more than two dozen bills were introduced in Congress in 2020 and 2021 alone.[15] The law faces criticism from all sides, with reform efforts being led by Democrats, Republicans, internet law scholars, and even many tech-industry executives.[16] On the fundamentals there is broad agreement: Section 230's core protections are essential to the modern internet and have enabled a vibrant online world that must be preserved; but that virtual world is also home to much wrongdoing and its levers of power are controlled by a small number of companies that Section 230 sometimes overprotects.[17] A more tailored immunity

E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 527–28 (2019) (noting Google and Facebook's capture of the digital advertising market in the United States and resultant effects on the traditional publishing industry).

13. *See* Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1952–53 (2019) (proposing modification to Section 230 immunity to spur platforms to action to protect against revenge porn and other invasions of sexual privacy); Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1755–59, 1795–804 (2019) (describing rising danger to privacy and security posed by advances in technology for creating deep fakes and noting that Section 230 limits legal recourse against online entities that distribute such fakes).

14. *See* Ann Bartow, *Internet Defamation as Profit Center: The Monetization of Online Harassment*, 32 HARV. J.L. & GENDER 383, 384 (2009) (tracing the rise of commercial reputation defense services to the lack of traditional avenues of recourse to respond to online harassment); Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1836–43 (2010) (sketching the vision for a new era of privacy law and noting the barrier that Section 230 poses to tortious enablement claims against online entities); Danielle Keats Citron & Benjamin Wittes, *The Problem Isn't Just Backpage: Revising Section 230 Immunity*, 2 GEO. L. TECH. REV. 453, 455–56 (2018) (proposing that online immunity be narrowed to allow claims against online entities that do not take reasonable steps to address unlawful third-party content); Benjamin Edelman & Abbey Stemler, *From the Digital to the Physical: Federal Limitations on Regulating Online Marketplaces*, 56 HARV. J. ON LEGIS. 141, 143 (2019) (noting the bar that Section 230 poses to the regulation of modern online marketplaces); Olivier Sylvain, *Intermediary Design Duties*, 50 CONN. L. REV. 203, 203 (2018) (suggesting that the online immunity doctrine be updated to consider the manner in which online entities elicit and use their users' data).

15. *See* Jess Miers, *Section 230 Bill Tracker*, https://docs.google.com/spreadsheets/d/16nl5RZUvowt0kuzAgd-7QF136jd1XvwYQ_IL6Cwk-QY (last visited Mar. 4, 2022) (tracking spreadsheet of proposed Section 230 amendments run by Jess Miers of jessmiers.medium.com).

16. *See infra* Section II.A.

17. *See infra* Sections I.B–II.A.

doctrine would be an improvement if it could be implemented without undermining the statute's other objectives.

Despite widespread agreement on basic principles, however, action from Congress is unlikely. New proposals crop up here, there, and everywhere, but none has been able to muster the support of a congressional majority. Deadlock on internet immunity is attributable to multiple factors. Most visible[18] is the two parties' focus on different aspects of the problem. Democrats prioritize protecting the public from harmful content such as falsified political ads, hate speech, and materials promoting terrorism, whereas Republicans prioritize correction of perceived political bias, alleging that platforms' content-censorship practices systematically silence conservative voices. Political polarization compounds the problem.[19] Even where the parties' concerns are compatible, compromise has been difficult because "free speech" and "online content moderation" have been deployed as partisan rallying cries rather than dually desirable policy goals.

Rather than add to the sizeable (and growing) body of literature proposing changes to Section 230, this Article tackles a different problem—how to achieve meaningful reform despite a decades-old internet immunity statute and a Congress unable to act. This Article shows how, even without fresh legislation from Congress, significant reform is possible via an unlikely source: the Section 230 internet immunity statute that is already on the books.[20] Although decades of judicial precedent have cemented in place an expansive interpretation of internet immunity that lacks the nuance to govern the modern virtual world, Section 230's sparse language—a mere twenty-six words—also contains the seeds for reform. An interpreter with a fresh slate could read the same statutory language to produce very different results. This Article shows how Section 230's linguistic indeterminacy opens an alternative path to reform. Judicial elaboration by state and federal courts[21] could reinterpret Section 230, without any change to the statutory language, to address the very problems that have been the focus of

18. Other reasons include the rapid pace of change in internet technology; the difficulty of drafting legislation in the abstract for future, unseen technologies; and Congress's limited competence, as a majority-ruled body of nonexperts, to move quickly to address technological change. *See infra* Sections II.B, III.A.

19. *See infra* Section II.B.1.

20. *See infra* Sections III.B–C.

21. *See infra* Sections III.B–C.

reform proposals: online wrongdoing, disparate treatment of online versus offline entities, content-moderation practices, and perceived censorship bias.

This Article approaches the problem in three parts. Part I begins with an overview of Section 230's design and continued importance before moving on to discuss the ways that Section 230, as currently interpreted, is insufficiently nuanced to govern the modern internet. Part II surveys proposed legislation and examines why Congress has been unable to act despite wide agreement regarding the dangers of overextending Section 230 immunity and the importance of preserving free expression. Finally, Part III proposes judicial elaboration of Section 230's sparse textual provisions to overcome congressional gridlock and achieve significant reform.

I. THE INTERNET'S AGING PROGENITOR

Section 230's importance to the modern internet is hard to overstate. The federalization of internet law and elimination of any obligation on online entities to moderate third-party content helped to fuel the internet's explosive growth from the 1990s through the 2000s, and its protections are critical to the internet's continued success in the decades to come. But the statute is starting to show its age. Although free expression and a robust online economy remain as important as ever, Section 230, and the tech industry it protects, has faced withering criticism for interfering with other private and governmental interests. Prominent members of both parties are now calling for reform, criticizing Section 230 and the entities it protects for failing to stop election interference and other public disinformation campaigns, censoring conservative political voices, and preventing victims of online harms from seeking redress.

This Part begins with an overview of Section 230's design and continued importance before moving on to discuss the ways in which Section 230, as currently interpreted, is a poor fit for the modern internet.

A. The Law that Created the Internet

Section 230 immunizes online entities against lawsuits related to content created by their users or other third parties.[22] The law

22. Importantly, although it bars most civil claims, Section 230 does not prevent criminal prosecution and expressly excludes from its protection any claims "pertaining to intellectual property." *See* 47 U.S.C. § 230(e).

promotes "decency" on the internet by allowing online entities to censor "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" content without fear of being "treated as the publisher or speaker" of—and held liable—for whatever content they fail to censor.[23] The law promotes freedom of expression by guaranteeing online entities' ability to receive and transmit the massive volume of information that flows into their systems without fearing liability based on the nature of its contents. By protecting online entities against liability for hosting or relaying content, the statute has supported the internet's growth in two related ways.

First, Section 230 shields online entities like Facebook or Twitter from an economically crippling duty to moderate the content flowing through their systems. Requiring such entities to review the millions of daily posts and remove unlawful material would impose an insurmountable logistical and financial burden and undermine the internet as we know it.[24] By immunizing online entities against lawsuits related to third-party content, Section 230 ensures that the costs of moderating user-created content do not stifle the growth of internet platforms.

Second, and relatedly, Section 230 protects against collateral censorship of users' speech. Were online entities at risk of legal liability whenever one of their users posted something unlawful, platforms might decide to block their users from posting even slightly risky material, to avoid the cost of moderating content and the risk of legal liability for failing to do so.[25] Why risk posting content that could subject the company to liability, when the platform, unlike the speaker herself, has no intrinsic interest in publicizing the message? Most likely to engage in widespread censorship would be platforms like Twitter, which transmit so much content that they could not possibly hope to screen it all. But the incentive to censor would press even low-volume sites, like individual blogs, whose operators typically lack the resources of

23. *See id.* § 230(c).

24. *See* Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. ON TELECOMM. & HIGH TECH. L. 101, 101–02 (2007) (noting the billions of web pages indexed by Google's search engine and observing that if it or other "Internet intermediaries were liable every time someone posted problematic content on the Internet, the resulting threat of liability and effort at rights clearance would debilitate the Internet").

25. Wu, *supra* note 11, at 298–300.

larger entities to respond to problematic material.[26] Without Section 230's protections, the legal risks of hosting user-created content would push entities of all sizes to dramatically alter their current practices. Platforms might require that users' posts be manually prescreened before becoming visible to the public; they might adopt automated censorship tools calibrated to let through only the most benign speech; or they might decide to eliminate user-created content from their sites altogether by removing comment-posting functionality. The result would be the elimination of decades of free speech advances built on inexpensive and free flowing internet publishing technologies.[27]

B. Section 230 Shows Its Age

But the venerable statute now shows its age. The Congress of 1996 did not foresee the internet of today, and Section 230 now presides over a very different internet from the one it was designed to govern. Section 230 assumes a publication-industry-like model of the internet. It encourages censorship, speaks in terms of "publishers or speakers" and "content providers,"[28] and is well suited to govern the internet's information repositories and communications channels—modern analogues to the publication world, like Facebook, Twitter, and Netflix. But publication has never been the internet's exclusive function, and it is even less so now than it was in 1996. Internet entities of today are much larger, diverse, and interactive and serve as platforms to support the delivery of innumerable real-world goods and services that would have been unimaginable twenty years ago. Authoring or failing to moderate content flowing through their services is not the only way that online entities can cause harm, and Section 230's bright-line rule relying on content authorship as the deciding factor for immunity is poorly tailored to the internet that exists today.

26. *See id.* at 301 (reasoning that the collateral censorship problem extends to both low- and high-volume intermediaries and that some of the highest value speech, like corporate whistleblowing, is risky for intermediaries and the most likely to be censored).

27. *See id.* at 298–99 (observing that pre-internet speech was "limited to those who were able to get past the old gatekeepers—newspapers, book publishers, retailers, and the like" but that "[n]ow all that is needed is an Internet connection."); *see also* Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805, 1806–07 (1995) (noting that historically, the right to free speech has favored popular or well-funded ideas, but predicting, presciently, that new information technologies would dramatically reduce the costs of distributing speech and create a more diverse and democratic environment).

28. *See* 47 U.S.C. § 230(c).

Critics of Section 230 point to four main problem areas. First, Section 230 includes no scienter-based limitation on immunity. An online entity is eligible for immunity even if it is aware of or even intends to cause the harms that result from its platform.[29] The statute was, for example, famously invoked to bar a sex-trafficking conspiracy claim asserted against the website Backpage.com by plaintiffs who alleged the site hosted "escort" ads of underage girls and intentionally obstructed law-enforcement efforts against sex traffickers so that it could continue to profit from the ad sales.[30] It has similarly protected online entities against claims for knowingly facilitating illegal gun sales,[31] distributing child pornography,[32] and other unlawful conduct, on the ground that, under Section 230, online entities are immune from claims related to third-parties' use of their platforms, regardless of knowledge or intent.

Second, Section 230 creates a disparity in the law's treatment of online versus offline entities in nonpublication contexts, such as product-defect claims and actions against online marketplaces. In such contexts, Section 230's content-authorship-based test for immunity is problematic because, although the plaintiff's injury may be causally connected with third-party-created content, the defendant's alleged wrongdoing often is not a failure by the defendant, as a publisher, to moderate that content. Applying Section 230 to nonpublication claims, courts have, for example,

29. *See id.* § 230(c)(1); *see also, e.g.*, Daniel v. Armslist, LLC, 926 N.W.2d 710, 726 (Wis. 2019) (explaining that the plaintiff's allegation that Armslist knew its website was used for illegal gun sales "does not change the result" because Section 230 "contains no good faith requirement" and "courts do not allow allegations of intent or knowledge to defeat a motion to dismiss").

30. Doe v. Backpage.com, LLC, 817 F.3d 12, 16–17 (1st Cir. 2016), *cert. denied*, 137 S. Ct. 622 (2017), *superseded by statute*, Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (FOSTA), Pub. L. No. 115-164, 132 Stat. 1253, *as recognized in* Teatotaller, LLC v. Facebook, Inc., 242 A.3d 814, 820 (N.H. 2020). Whether criminal enforcement and Congress's later amendment of Section 230 to permit civil claims benefited sex workers is an open question. Some fear that criminalization and other legal barriers to sex work may harm sex workers by forcing them to work in secret, more dangerous environments. *See* Anna North, *Sex Workers Are in Danger. Warren and Sanders Are Backing a Bill That Could Help*, VOX (Dec. 17, 2019, 12:20 PM), https://www.vox.com/identities/2019/12/17/21024859/sex-work-bernie-sanders-elizabeth-warren-fosta.

31. *See Daniel*, 926 N.W.2d at 714, 716 (barring negligence, public nuisance, wrongful death, aiding and abetting tortious conduct, and other claims against Armslist, alleging that it intentionally designed its website to facilitate illegal gun sales).

32. *See* Doe v. Am. Online, Inc., 783 So. 2d 1010, 1011–12, 1018 (Fla. 2001) (finding Section 230 to bar action against AOL for violating Florida statutes prohibiting distribution of child pornography despite allegation that AOL was aware that a particular user of its service was transmitting unlawful photographs and yet declined to intervene).

dismissed product-defect claims against Grindr[33] and Snapchat[34] for failing to incorporate safety features into their apps, and unfair competition claims against Facebook[35] and Google[36] for making false claims about their products or failing to abide by their stated terms of service.

Third, Section 230 enables online platforms to freely disseminate harmful or offensive material. The statute eliminates any duty on Facebook, Twitter, and other internet entities to review or censor content created by their users, regardless of how harmful dissemination of that content may be to society. Online platforms have come under increasing criticism for the harmful content that they host, including election misinformation,[37] hate speech,[38]

33. Herrick v. Grindr, LLC, 306 F. Supp. 3d 579, 584, 590–91 (S.D.N.Y. 2018), *aff'd*, 765 F. App'x 586 (2d Cir. 2019) (finding dating app immune under Section 230 despite inclusion of geolocation function and lack of safety features which allowed user's ex-boyfriend to harass him).

34. Lemmon v. Snap, Inc., 440 F. Supp. 3d 1103 (C.D. Cal. 2020), *rev'd and remanded*, 995 F.3d 1085 (9th Cir. 2021) (discussing a negligence claim against Snapchat for alleged defects in design of the speed filter feature of its app, which plaintiff alleged contributed to auto accidents).

35. Caraccioli v. Facebook, Inc., 700 F. App'x 588, 590 (9th Cir. 2017) (affirming dismissal of unfair competition claim alleging Facebook violated its own terms of service to plaintiff's detriment by failing to block obscene videos of plaintiff posted to the service by an unknown person).

36. Marshall's Locksmith Serv. Inc. v. Google, LLC, 925 F.3d 1263, 1265–66, 1272 (D.C. Cir. 2019) (affirming dismissal of the Lanham Act false advertising claims of locksmith companies which alleged that Google and other online advertising platforms had "conspired to 'flood the market' of online search results with information about so-called 'scam' locksmiths, in order to extract additional advertising revenue" from truly local locksmiths).

37. *See* Kevin Roose, *Reviewing Misinformation: What Reporters and Readers Found*, N.Y. TIMES, Nov. 5, 2018, at A16 (discussing numerous examples of election misinformation spread on Facebook, Twitter, and other platforms).

38. *See* Mike Isaac, *Facebook Lets Hate Flourish, Report Finds*, N.Y. TIMES, July 9, 2020, at A1 (detailing findings of report from internal audit commissioned by Facebook that faulted it for endangering civil rights by allowing hateful and violent speech on its platform); Daisuke Wakabayashi, *Why Hate Speech on the Internet Is a Never-Ending Problem*, N.Y. TIMES, Aug. 6, 2019, at B1 (discussing the issue of hate speech on internet platforms and proposals to reform Section 230).

revenge porn,[39] and false information about COVID-19.[40] They have also faced criticism for platform-design and content-moderation decisions that have enabled cyber stalking, cyber bullying,[41] and facilitated terrorism-related activity in violation of civil antiterrorism laws.[42] Because, under Section 230, a platform has no legal obligation to review user content, any moderation decision is at its discretion and immune from legal challenge.

Fourth, and relatedly, Section 230 insulates online platforms from legal challenges even if their content-moderation policies are politically biased or disfavor marginalized voices. Some critics perceive systematic biases in the way that platforms' content-moderation policies select users' posts for promotion, demotion, or censorship.[43] Most prominently, many conservatives criticized Twitter and Facebook for their decisions to disable former

39. *See* Erica Goode, *Once Scorned, but on Revenge Sites, Twice Hurt*, N.Y. TIMES, Sept. 24, 2013, at A11 (discussing the problem of revenge porn and efforts to criminalize it); *see also* People v. Austin, 2019 IL 123910 (2019), *cert. denied sub nom.* Austin v. Illinois, No. 19-1029, 2020 WL 5882221 (U.S. Oct. 5, 2020) (upholding Illinois revenge porn law as not improperly restricting freedom of speech). *See generally* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345 (2014) (describing the problem of nonconsensual distribution of private sexual images and arguing for the criminalization of revenge porn).

40. *See* Mike Isaac, *Facebook to Remove Vaccine Misinformation*, N.Y. TIMES, Dec. 4, 2020, at A9 (discussing Facebook's voluntary shift to begin removing misinformation about COVID-19 after facing criticism for false information distributed through its platform).

41. *See* Maeve Duggan, *Online Harassment 2017*, PEW RSCH. CTR. (July 11, 2017), https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/ (poll finding 41% of Americans to have been subjected to harassing behavior online); Jessica M. Goldstein, *Reeling from 'Revenge Porn'*, WASH. POST, Nov. 4, 2020, at C1 (discussing domestic abusers' threats of disclosing intimate images to control partners); *see also* Herrick v. Grindr, LLC, 306 F. Supp. 3d 579, 590 (S.D.N.Y. 2018), *aff'd*, 765 F. App'x 586 (2d Cir. 2019) (describing harassment of former romantic partner via Grindr app).

42. *See* Tony Romm, Rachel Lerman, Cat Zakrzewski, Heather Kelly & Elizabeth Dwoskin, *Lawmakers Clash with Silicon Valley CEOs on Liability*, WASH. POST, Oct. 29, 2020, at A21 (discussing Senate questioning of tech company leaders regarding their content-moderation practices for content including terrorist propaganda); *see also* Force v. Facebook, Inc., 934 F.3d 53, 68–72 (2d Cir. 2019) (rejecting claim alleging platform's material support of terrorism); Fields v. Twitter, Inc., 217 F. Supp. 3d 1116, 1118 (N.D Cal. 2016) (dismissing case pursuant to Section 230 suit alleging Twitter knowingly provided material support to terrorist group), *aff'd on other grounds*, 881 F.3d 739 (9th Cir. 2018).

43. *See* Kate Conger & Davey Alba, *Admirers Follow President into Battle with Twitter*, N.Y. TIMES, May 28, 2020, at B1 (describing conservatives' criticism of Twitter for adding critical fact-check labels to tweets of President Trump); Tony Romm, *Trump Considers 'Legal Steps' Against Social Media Sites*, WASH. POST, Sept. 24, 2020, at A20 (discussing proposal by President Trump to reform Section 230 in response to perceived political bias of online platforms).

President Trump's media accounts[44] and to restrict access to a series of stories published by the *New York Post* about President Joe Biden's son, Hunter.[45] Google and other content aggregators have faced similar criticism of algorithmic bias against the poor, women, and racial and other minorities because the algorithms they rely on to curate and analyze online content may perpetuate social stereotypes and inequalities.[46] As online communication has become the preferred format for political discourse, those who feel excluded from the conversation have little recourse.

* * *

The internet has changed since Section 230 was enacted in 1996. The tech world is much broader and more mature. And internet speech is now controlled by a small number of key players who, as private entities, moderate content at their discretion, free from public scrutiny. Yet, as online rather than physical-world entities, they enjoy a preferred legal status under Section 230 that insulates their decisions from legal challenge.[47]

II. ACADEMIC BORBORYGMI[48] AND CONGRESSIONAL DEADLOCK

Although Section 230 continues to play a critical role governing internet liability, its defects have put it at the center of public debate

44. *See* Kevin Roose, *Megaphone to Masses Goes Silent*, N.Y. TIMES, Jan. 8, 2021, at B1 (discussing Twitter's and Facebook's decisions to disable the President's accounts after the attack on the U.S. Capitol).

45. *See* Kevin Roose, *Eyes on 2016, Social Media Tackles 2020*, N.Y. TIMES, Oct. 16, 2020, at A1 (recounting the incident and observing that such incidents put social media companies "in a precarious spot" because they "are criticized when they allow misinformation to spread" and also "when they try to prevent it").

46. *See* Farhad Manjoo, *Search Bias, Blind Spots and Google*, N.Y. TIMES, Aug. 31, 2018, at B1 (recounting examples of algorithmic bias, such as Google's spelling correction of the search "English major who taught herself calculus" to "taught *himself* calculus").

47. *See generally* Klonick, *supra* note 10 (detailing the pivotal role online entities play in controlling public discourse and their processes for content-moderation decision making); *see also* Caraccioli v. Facebook, Inc., 700 F. App'x 588, 590 (9th Cir. 2017) (affirming dismissal under Section 230 of unfair competition claim alleging Facebook violated its own terms of service to plaintiff's detriment by failing to block obscene videos of plaintiff posted to the service).

48. "Borborygmi" is a fancy-pants word I once heard a physician use to describe stomach gurgles. Despite my gut intuition, the word appears, somewhat disappointingly, not to be onomatopoeic. *See Borborygmi*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY (11th ed. 2003) (defining the word as "intestinal rumbling caused by moving gas" and tracing its etymology to the Greek *borboryzein*, meaning "to rumble"). It seems an apt descriptor for legal scholars' ruminations.

over internet policy. The law faces critics on all sides, with calls for reform coming from leading Democrats, Republicans, internet law scholars, and even tech-industry executives.[49] Some urge complete repeal;[50] others suggest targeted amendments;[51] and still others argue that its defects are overblown, that changes are likely to do more harm than good, and that the statute should be left as is.[52] Even for those who think Section 230 should be changed, however, there is little agreement on particular legislative or regulatory changes.

This Part summarizes numerous recent proposals to reform Section 230, many of which are currently pending before Congress, and explores why, despite broad support for change, Congress has been unable to act.

A. Proposals for Section 230 Reform

One collection of proposals would amend Section 230 to curtail immunity for online entities that intentionally facilitate unlawful conduct. For example, a Department of Justice review of Section 230 concluded that a "Bad Samaritan" carve out[53] should be added to

49. *See* Dave McCabe, *Tech Giants Shift Posture on Legal Shield*, N.Y. TIMES, Dec. 16, 2020, at B1 (discussing reform pressure from political leaders and shift by Facebook, Twitter, Snap, and others to support modifications to Section 230).

50. Though their reasons differ, both President Biden and former President Trump have voiced support for complete repeal of Section 230. *See* John D. McKinnon & Ryan Tracy, *Where Trump and Biden Stand on Big Tech; Both See Problems, but Differ on Solutions*, WALL ST. J., Sept. 17, 2020, at A4 ("Mr. Biden surprised the tech world when he called for revoking Section 230. But unlike conservatives, Mr. Biden says some social-media platforms do too little policing, not too much.").

51. *See infra* Section II.A; *see also* Gregory M. Dickinson, *Rebooting Internet Immunity*, 89 GEO. WASH. L. REV. 347, 381–85 (2021) (surveying recent proposed reforms to Section 230 and assessing risks and limitations of those reforms).

52. *See, e.g.*, Goldman, *supra* note 11, at 36-46 (arguing that Section 230's enhanced substantive and procedural protections for online entities beyond those of the First Amendment counsel against reform); Riana Pfefferkorn, *House Introduces EARN IT Act Companion Bill, Somehow Manages to Make It Even Worse*, THE CTR. FOR INTERNET & SOC'Y (Oct. 5, 2020), http://cyberlaw.stanford.edu/blog/2020/10/house-introduces-earn-it-act-companion-bill-somehow-manages-make-it-even-worse (discussing proposed legislation to reduce scope of Section 230 immunity).

53. *See* U.S. DEP'T OF JUST., SECTION 230—NURTURING INNOVATION OR FOSTERING UNACCOUNTABILITY? 3, 14–15 (2020), available at https://www.justice.gov/file/1286331/download [hereinafter DOJ SECTION 230 RECOMMENDATIONS]. In recommending a Bad Samaritan carve out, the DOJ referenced Daniel v. Armslist, LLC, 926 N.W.2d 710 (Wis. 2019), noting that, in that case, the website that facilitated the sale of a firearm to a prohibited person "was immune under Section 230, despite allegations that [the] website was intentionally designed with the specific purpose of skirting federal firearm laws." DOJ SECTION 230 RECOMMENDATIONS, *supra*, at 14.

the statute to ensure that online entities that purposefully solicit "third parties to sell illegal drugs to minors, exchange child sexual abuse material," or engage in other unlawful activities through their platforms "do not benefit from Section 230's sweeping immunity at the expense of their victims."[54] A host of proposed amendments introduced in Congress in 2020 would strip immunity from online entities that facilitate such behavior.[55] Academic commentators have offered their own solutions, such as limiting immunity to claims that impose a content-moderation burden on defendants,[56] applying joint enterprise liability theory to allow claims against entities that intentionally profit from their users' misconduct,[57] and imposing a reasonableness requirement that would require online entities to take reasonable steps to prevent misuse of their services to qualify for immunity.[58] These and other similar proposals are all motivated by the perceived overprotection of online entities under Section 230, but they differ in the types of misconduct they target and the enforcement mechanisms they employ.

Another set of proposals seeks to combat online dissemination of harmful and offensive material, such as political misinformation, hate speech, child pornography, and posts promoting violent extremism. These proposals would spur online platforms to police

54. DOJ SECTION 230 RECOMMENDATIONS, *supra* note 53, at 14.

55. *See, e.g.*, Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (EARN IT Act), S. 3398, 116th Cong. (2020) (allowing civil suits against companies that recklessly distribute child pornography); See Something, Say Something Online Act of 2020, S. 4758, 116th Cong. (2020) (requiring online entities to report to the federal government criminal activity on their platforms of which they are aware or reasonably should have been aware and stripping Section 230 immunity where an entity fails to do so).

56. *See* Dickinson, *supra* note 51, at 390–95.

57. *See* Agnieszka McPeak, *Platform Immunity Redefined*, 62 WM. & MARY L. REV. 1557 (2021); *see also* Olivier Sylvain, *Intermediary Design Duties*, 50 CONN. L. REV. 203, 276–77 (2018) (suggesting online immunity doctrine should consider entities' intentional solicitation and sale or use of user data).

58. *See* Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, 86 FORDHAM L. REV. 401, 419 (2017); *see also* Citron & Wittes, *supra* note 14, at 455–56 (arguing immunity should be limited to online entities that, when warned, take reasonable steps to protect against illegal activity); Benjamin Edelman & Abbey Stemler, *From the Digital to the Physical: Federal Limitations on Regulating Online Marketplaces*, 56 HARV. J. ON LEGIS. 141, 193 (2019) (contending immunity should be denied, among other times, when entities were on actual notice of a specific pattern or problem); Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335 (2005) (arguing no immunity where an entity has actual notice of ongoing unlawful activity); Tushnet, *supra* note 11, at 1010 (holding immunity could be denied where an entity refuses to remove content if the original speaker has conceded liability).

content on their platforms by withholding Section 230's protections unless they bar certain types of speech and activity. For example, the Protecting Americans from Dangerous Algorithms Act would withhold immunity from online platforms whose algorithms amplify content related to international terrorism and certain civil rights violations.[59] Similarly, the Holding Sexual Predators and Online Enablers Accountable Act would exclude from immunity online platforms that recklessly facilitate or host content depicting child sexual exploitation.[60] Many other proposals take this same basic form: Repeal or narrow Section 230 immunity to drive online platforms to adopt more stringent content-moderation policies.[61]

Finally, a third set of proposals attacks the opposite problem—platforms' perceived censorship or marginalization of particular groups and individuals, especially political conservatives and racial minorities. These proposals would reduce or eliminate online entities' discretion to selectively bar or promote certain speech from their platforms. For example, the Protecting Constitutional Rights from Online Platform Censorship Act would combat content-moderation bias by amending Section 230 to create a private right of action against any online platform that removes or restricts access to content protected by the First Amendment.[62] Similarly, the Biased Algorithm Deterrence Act would target platforms' promotion and demotion of select user content by withholding Section 230 immunity for claims against online entities that stem from user-created content that the entity reordered to appear other than as chronologically posted.[63] Although the proposals in this group differ dramatically in their particulars, all attempt to curb content-moderation practices that may interfere with the free expression of disfavored groups.[64]

59. *See* Protecting Americans from Dangerous Algorithms Act, H.R. 8636, 116th Cong. (2020).

60. *See* Holding Sexual Predators and Online Enablers Accountable Act of 2020, S. 5012, 116th Cong. (2020).

61. *See, e.g.*, Curbing Abuse and Saving Expression in Technology Act (CASE-IT Act), H.R. 285, 117th Cong. (2021) (among other things, withholding immunity for entities that knowingly facilitate distribution of obscene content to minors); Cecilia Kang, David McCabe & Jack Nicas, *For Tech, Not Much to Celebrate*, N.Y. TIMES, Nov. 11, 2020, at B1 (noting that President Biden's "clearest position on internet policy" has been to revoke Section 230, which protects tech companies "from lawsuits for hosting or removing harmful or misleading content").

62. *See* Protecting Constitutional Rights from Online Platform Censorship Act, H.R. 83, 117th Cong. (2021).

63. *See* Biased Algorithm Deterrence Act of 2019, H.R. 492, 116th Cong. (2020).

64. *See, e.g.*, Limiting Section 230 Immunity to Good Samaritans Act, H.R. 8596, 116th Cong. (2020) (requiring platforms to adhere to stated terms of service regarding content-

B. Hyperactive Inaction in Congress

Despite a tsunami of proposed legislation and widespread support for change, Congress is at a standstill. On the fundamentals, there is broad agreement: (1) Section 230's protections have been essential to the creation of the modern internet; (2) online platforms enable a new form of democratic self-expression that must be preserved; but (3) the virtual world has also come to harbor or even foster all variety of human wrongdoing; and (4) when Section 230 impedes legal action against such wrongdoing, it is at best a necessary evil. Put differently, Section 230 must be preserved insofar as it protects a critical medium of expression. Nobody wants to go back to the dark ages of the 1980s by allowing platforms to be sued out of existence or forced to curtail user speech. But Section 230's broad immunity provisions sometimes protect bad actors along with the good, and a more tailored immunity doctrine would be an improvement if it could be implemented without undermining the statute's objectives.

Widespread agreement on basic principles, even at this high level of generality, would often produce a legislative solution—uniting legislators around those goals most central to a governing majority. Indeed, that is exactly what happened in 2018 when Congress amended Section 230 by enacting the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA).[65] So troubled was Congress by the First Circuit's dismissal of a sex trafficking conspiracy claim against the website Backpage.com[66] that, despite

moderation practices to qualify for immunity); Online Freedom and Viewpoint Diversity Act, S. 4534, 116th Cong. (2020) (eliminating immunity where a platform editorializes or modifies third-party content); Stopping Big Tech's Censorship Act, S. 4062, 116th Cong. (2020) (removing immunity for entities that limit access to "constitutionally protected material"); Ending Support for Internet Censorship Act, S. 1914, 116th Cong. (2020) (requiring politically neutral content-moderation practices to qualify for immunity); Abandoning Online Censorship (AOC) Act, H.R. 8896, 116th Cong. (2020) (repealing Section 230 "to stop censorship, and for other purposes"); Protect Speech Act, H.R. 8517, 116th Cong. (2020) (requiring platforms to publish and adhere to terms of service governing content-moderation practices to qualify for Section 230 protection); Stop the Censorship Act of 2020, H.R. 7808, 116th Cong. (2020) (replaces with "unlawful" the vague "otherwise objectionable" category of content removal that qualifies for Section 230(c)(2) "Good Samaritan immunity").

65. *See* Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, 132 Stat. 1253 (2018).

66. *See* Doe v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016), *cert. denied*, 137 S. Ct. 622 (2017), *superseded by statute*, Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), Pub. L. 115-164, 132 Stat. 1253, *as recognized in* Teatotaller, LLC v. Facebook, Inc., 242 A.3d 814, 820 (N.H. 2020).

great respect for Section 230's speech-protecting function, overwhelming majorities in the House and Senate revised Section 230 to specifically exclude sex trafficking claims.[67] Since 2018, however, no additional legislative action appears likely, even though Congress and academic commentators widely acknowledge both the dangers of overextending immunity and the importance of preserving free expression online.

1. Political Polarization

Congressional deadlock on internet immunity is attributable to multiple factors. Most visibly, the two parties focus on different aspects of the problem. Democrats criticize online platforms' failure to protect the public from harmful content such as falsified political ads, hate speech, and materials promoting terrorism,[68] whereas Republicans focus on perceived political bias, alleging that platforms' content censorship practices systematically silence conservative voices.[69] To some extent, these concerns are irreconcilable: Republicans can hardly be expected to consent to the targeting of conservative speech, nor Democrats to election interference and the incitement of violence. But political polarization compounds the problem. A shrinking moderate center in Congress leaves fewer members likely to cross the aisle to craft bipartisan legislation.[70] And to the similarly polarized public that

67. *See, e.g.*, 163 CONG. REC. S4671 (daily ed. Aug. 1, 2017) (statement of Sen. Portman, R-Ohio, speaking on behalf of bipartisan group of senators introducing the bill that would become FOSTA) ("I believe that we need to have free internet. All of us do. I believe that the Communications Decency Act is a well-intentioned law that has an important purpose. But the law was not intended to protect those who willingly facilitate illegal conduct . . . ."); 164 CONG. REC. H1278 (daily ed. Feb. 27, 2018) (statement of Rep. Wagner, R-Missouri) (describing FOSTA as "in many ways just a simple statement of the obvious: Congress does not believe—and did not ever believe—that rape was a perquisite [sic] of a free and open internet"); 164 CONG. REC. S1852 (daily ed. Mar. 21, 2018) (statement of Sen. Heitkamp, D-North Dakota) ("This was not easy. No one should think that this came together easily or that we didn't have many moments where we did our own soul-searching, those of us who are committed to the First Amendment and those of us who are committed to free access of means to express our opinions and do our business.").

68. *See* Tony Romm & Elizabeth Dwoskin, *Silicon Valley Braces for Regulatory Change*, WASH. POST, Jan. 19, 2021, at A1 (discussing Democrats' and President Biden's efforts to press online platforms to censor online content).

69. *See* Tony Romm, *GOP Votes to Subpoena Facebook, Twitter CEOs*, WASH. POST, Oct. 23, 2020, at A16 (discussing the Republicans' "campaign to rethink Section 230" "in response to concerns about political bias").

70. *See* Michael S. Kang, *Hyperpartisan Gerrymandering*, 61 B.C. L. REV. 1379, 1419 (2020) (surveying recent political science literature on political polarization and attributing that

make up their representatives' constituencies, cooperation and compromise would be defeat.[71] Even where the parties' concerns are compatible, compromise is challenging because "free speech" and "online content moderation" have become partisan rallying cries rather than dually desirable policy objectives.[72]

2. Congress and Technological Change

Congress's inaction is also, in part, a natural response to the difficulty of crafting legislation to govern a rapidly evolving field. For decades, Congress has struggled to keep pace with the constantly changing technological landscape, from automobiles and nuclear power plants to the internet and smartphones.[73] The public exerts continual pressure to respond to headlines, which limits Congress's capacity to develop detailed, long-term legislative solutions.[74] And even when it has the time and political support to do so, members of Congress often lack the expertise[75] to

polarization in part to political gerrymandering that produces fewer contested districts and moderates).

71. *See generally* David E. Pozen, Eric L. Talley & Julian Nyarko, *A Computational Analysis of Constitutional Polarization*, 105 CORNELL L. REV. 1 (2019); Nicholas O. Stephanopoulos, *The Dance of Partisanship and Districting*, 13 HARV. L. & POL'Y REV. 507 (2019); Richard H. Pildes, *Why the Center Does Not Hold: The Causes of Hyperpolarized Democracy in America*, 99 CALIF. L. REV. 273, 276 (2011).

72. *See* Emily A. Vogels, Andrew Perrin & Monica Anderson, *Most Americans Think Social Media Sites Censor Political Viewpoints*, PEW RSCH. CTR. (Aug. 19, 2020), https://www.pewresearch.org/internet/2020/08/19/most-americans-think-social-media-sites-censor-political-viewpoints (finding 90% of Republicans and 59% of Democrats believe it is likely that social media sites intentionally censor political viewpoints they disfavor and that 71% of Republicans compared to 25% of Democrats disapprove of social media sites labeling posts from elected officials as misleading or inaccurate).

73. *See generally* Jody Freeman & David B. Spence, *Old Statutes, New Problems*, 163 U. PA. L. REV. 1 (2014); Wulf A. Kaal & Robert N. Farris, *Innovation and Legislation: The Changing Relationship – Evidence from 1984 to 2015*, 58 JURIMETRICS J. 303, 304 (2018); Albert C. Lin, *Revamping Our Approach to Emerging Technologies*, 76 BROOK. L. REV. 1309 (2011).

74. *See* Lin, *supra* note 73, at 1327.

75. Recognizing its own shortcoming, Congress in 1972 established the Office of Technology Assessment (OTA) to "equip [the legislative branch] with new and effective means for securing competent, unbiased information concerning the physical, biological, economic, social, and political effects of [technology]" and to use such information to provide "legislative assessment of matters pending before the Congress." Technology Assessment Act of 1972, Pub. L. No. 92-484, § 2, 86 Stat. 797 (1972) (codified at 2 U.S.C. §§ 471–81). Congress abolished the OTA in 1995 by cutting off its funding. It may be time to reconsider that decision. *See* Kevin Kosar, *Congress's Tech Policy Knowledge Gap*, CATO UNBOUND (June 10, 2019), https://www.cato-unbound.org/2019/06/10/kevin-kosar/congresss-tech-policy-knowledge-gap (discussing the OTA's purpose and advocating for its revival); Patrick Healy & Cornelia Dean, *Clinton Says She Would Shield Science from Politics*, N.Y. TIMES, Oct. 5,

understand and regulate complex technological issues and are likely to be heavily influenced by industry lobbyists and other beneficiaries of the status quo.[76]

These pressures can be seen in Congress's relationship with Section 230. Spurred to action in 1995 by the concern of the moment, internet pornography, Congress enacted the Communications Decency Act to limit children's access to online pornography by making it unlawful for entities to knowingly make "indecent" material available to minors.[77] Tacked on to this much more comprehensive Act[78] was Section 230, which supported the CDA's goal to protect the nation's children from pornography by ensuring that online entities would not risk incurring legal liability for any steps they might take to filter indecent material.[79] The provision underwent little analysis, deliberative process, or public debate, for Section 230 regulated an internet industry then so small that it attracted no significant attention.[80] Instead, Section 230 was crafted by a small group "flying by the seats of [their] pants"[81] and slipped through the legislative process virtually unnoticed.

After the internet-pornography emergency that brought Section 230 to life, congressional and public interest waned. It was not until 2018 that Congress revisited the statute. That year, as discussed previously, Congress responded to a new controversy—online sex trafficking on the Backpage.com website—by enacting FOSTA, which narrowly amended Section 230's immunity provisions[82] so that it could not be invoked as a defense to civil sex

2007, at A22 (reporting then-Senator and Democratic presidential candidate Hillary Clinton's call in 2007 for Congress to revive the OTA).

76. *See* Lin, *supra* note 73, at 1327–28. The advent of the internet age has placed even more pressure on legislative structures, perhaps outpacing regulatory capacity. Since 1998, the pace of innovation has accelerated and diverged from its historically parallel relationship with legislative and regulatory expansion. *See* Kaal & Farris, *supra* note 73, at 305.

77. *See* Communications Decency Act of 1996, Pub. L. 104-104, 110 Stat. 56 (1996) (relevant provisions codified at 47 U.S.C. § 223), *declared unconstitutional as to indecent material*, Reno v. Am. Civil Liberties Union, 521 U.S. 844, 883 (1997); *see also* KOSSEFF, *supra* note 3, at 61–63.

78. Few media outlets included any discussion of Section 230 in their coverage of the CDA. *See* KOSSEFF, *supra* note 3, at 66–68 (recounting the history of Section 230's enactment).

79. *See* 47 U.S.C. § 230; *supra* Section I.A.

80. *See* KOSSEFF, *supra* note 3, at 67–71.

81. *See id.* at 66.

82. See 47 U.S.C. § 230(e)(1), which FOSTA amended to exclude from Section 230's protections actions to enforce "[chapter] 110 (relating to sexual exploitation of children) of Title 18."

trafficking conspiracy claims.[83] FOSTA was to be the start of a new trend. Internet immunity reform proposals now regularly spring up to respond to the crises of the moment. With the internet having come to dominate so much of our political and social lives, Congress faces continuous calls to address a never-ending series of hot-button issues: Russian interference in the 2016 election,[84] the spread of medical and political misinformation on the internet,[85] biased content-moderation practices,[86] and the "de-platforming" of political speakers.[87] Unlike 1995, however, internet-related legislation must now run the gauntlet of opposition and lobbying efforts from a fully mature tech industry.[88] Congress faces

83. In its *Backpage* decision, the First Circuit interpreted Section 230 to immunize the Backpage website from a sex trafficking conspiracy claim brought pursuant to the Trafficking Victims Protection Reauthorization Act (TVPRA) of 2017 by underage girls who had become victims of sex trafficking and advertised for sale on the website. *See* Doe v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016), *cert. denied*, 137 S. Ct. 622 (2017), *superseded by statute*, Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), Pub. L. 115-164, 132 Stat. 1253, *as recognized in* Teatotaller, LLC v. Facebook, Inc., 242 A.3d 814, 820 (N.H. 2020).

84. *See, e.g.*, David D. Kirkpatrick, *Is Facebook Just a Platform? A Lawyer to the Stars Says No*, N.Y. TIMES, May 23, 2018, at A9 (discussing Russia's attempt to influence the 2016 election via social media and potential legislation from Congress that would require them to disclose buyers of political advertising).

85. *See, e.g.*, David McCabe, *Tech Giants Shift Posture on Legal Shield*, N.Y. TIMES, Dec. 16, 2020, at B1 (describing apparent strategic about-face of some leaders in the tech industry following sustained criticism for, among other things, failing to stop the spread of misinformation online); Health Misinformation Act of 2021, S.2448, 117th Cong. (2021) (would amend Section 230 to treat entities as publishers of health misinformation on their platforms if their service algorithmically amplified circulation of the content during a public health emergency).

86. *See, e.g.*, Kate Conger & Mike Isaac, *Adding Fact-Check Labels, Twitter Defies the President*, N.Y. TIMES, May 29, 2020, at B1 (discussing Twitter's decision to label some of former President Trump's tweets as misleading and the controversy over perceived political bias in social media platforms' content-moderation decisions); Disincentivizing Internet Service Censorship of Online Users and Restrictions on Speech and Expression Act ("DISCOURSE Act"), S.2228, 117th Cong. (2021) (would amend Section 230 to eliminate immunity where a platform moderates, modifies, or amplifies user posts).

87. *See, e.g.*, Elizabeth Dwoskin & Crag Timberg, *Dramatic Drop in Misinformation Online Amid Bans*, WASH. POST, Jan. 17, 2021, at A17 (discussing the policy debate surrounding former President Trump's suspension from Twitter and Facebook); NetChoice, LLC v. Paxton, No. 1:21-CV-840-RP, 2021 WL 5755120, at *15 (W.D. Tex. Dec. 1, 2021) (preliminarily enjoining enforcement of Texas HB20 law, that would prohibit online platforms from censoring users based on the viewpoint of their speech); NetChoice, LLC v. Moody, 546 F. Supp. 3d 1082, 1094 (N.D. Fla. 2021) (barring enforcement of Florida's SB 7072 law, which would treat social media platforms like common carriers and require them to host user speech of all viewpoints).

88. Facebook's lobbying expenditures have risen dramatically, from a mere $200,000 and two lobbyists as recently as 2009, to $20 million and 72 lobbyists in 2021. *See Meta*

tremendous pressure to act, but, apart from sex trafficking, no issue has held the staying power or built the momentum necessary to produce even minor change, let alone comprehensive reform.

3. Legislating in the Abstract

There is also a more fundamental obstacle to internet immunity reform: Congress's legislative infrastructure is poorly suited to address the sorts of disruptive technologies that increasingly demand its attention. The traditional legislative process is principally reactive. When a new problem arises, Congress responds by collecting data, deliberating to identify available options and form a consensus, and, finally, by attempting to craft an optimal, forward-looking rule to govern future instances of that problem.[89] Congress's response to *Backpage.com* is a good example. An apparent hole in sex trafficking civil remedies arose, and Congress enacted FOSTA to target the problem.[90] This approach to lawmaking ably governs future instances of well-understood problems, but it is less effective in environments of rapid and unpredictable change, where new problems may arise, only to be replaced by still newer ones before Congress can effectively respond.[91]

In a sense, of course, none of this is new. Lawmakers have long recognized that times change and that laws enacted to address one set of circumstances may eventually be called upon to govern a

Lobbying Profile, OPENSECRETS (2021), https://www.opensecrets.org/federal-lobbying/clients/summary?cycle=2021&id=D000033563. Facebook and Amazon are now the top corporate spenders on political lobbying in the United States. *See* Ilya Banares, *Facebook and Amazon Unleash Spending, Vault Atop U.S. Lobbying*, BLOOMBERG (Mar. 24, 2021), https://www.bloomberg.com/news/articles/2021-03-24/facebook-amazon-edge-out-other-corporate-giants-in-lobby-spend; *see also* Tom Jackman, *Tech Companies Push Back as Congress Tries to Fight Online Sex Trafficking*, WASH. POST (Sept. 18, 2017), https://www.washingtonpost.com/news/true-crime/wp/2017/09/18/tech-companies-push-back-as-congress-tries-to-fight-online-sex-trafficking/ (describing Google, Facebook, and others' opposition to the bill that eventually became FOSTA, and a letter to Congress describing the law as "a mistake of historic proportions").

89. *See* Wulf A. Kaal & Erik P.M. Vermeulen, *How to Regulate Disruptive Innovation-from Facts to Data*, 57 JURIMETRICS J. 169, 170–73 (2017) (discussing the traditional ex post rulemaking process and the challenge it faces when regulating rapidly evolving technology).

90. *See* Pub. L. 115-164, 132 Stat. 1253 (2018).

91. *See* Kaal & Vermeulen, *supra* note 89, at 173 (observing that in an environment of rapidly evolving innovation, "by the time legal issues are addressed, new and different legal issues are created").

much different future.[92] To account for this, legislation can be drafted broadly, to cover future as well as existing technologies or to require a specified standard of care regardless of circumstances. For example, when New York City established the Taxi & Limousine Commission in 1971, it established regulations to govern not Checker A11 taxicabs specifically, but any "motor vehicle, yellow in color, bearing a Medallion indicating that it is licensed . . . to carry up to five passengers for hire."[93] So drafted, preferences for improved fuel economy, the rise of the Honda Civic, and even electric motors posed no problem. The rule continued as it always had. But this approach has its limitations. Who, in 1971, could have imagined the internet, pocket-sized smartphone computers, and ridesharing apps that would one day throw the industry into chaos?[94] Lawmakers do their best to imagine the future and legislate at an appropriate level of abstraction. But sometimes the future brings unforeseeable shifts in technology, consumer behavior, or industry practices that render well-intentioned legislation ineffective or even harmful. Section 230 itself is a good example: a statute designed for ISPs and content distributors on the publication-centric internet of 1996 now struggles to govern the smartphone apps and online services of the modern virtual world.[95]

Given the pace of technological change and the difficulty of predicting—let alone legislating for—future innovation, it is no surprise that Congress has been cautious. Crafting abstract legislation to govern a world one has never seen is fraught with danger. In the current political climate, and with the fear of enacting legislation that only makes matters worse, it is no surprise that Congress has been unable to build the consensus required for comprehensive reform.

92. *See* Jody Freeman & David B. Spence, *Old Statutes, New Problems*, 163 U. PA. L. REV. 1, 3 (2014) (collecting and discussing the "significant literature on statutory 'obsolescence,' dating to the 1920s").

93. NEW YORK CITY, N.Y., RULES, Tit. 35, § 51-03 (Am. Legal Publ'g through Jan. 22, 2022).

94. *See* Mike Isaac, *Uber Hires Ex-Adviser to Obama*, N.Y. TIMES, Aug. 20, 2014, at B1 (discussing the state of regulatory confusion that followed the introduction of the Uber and Lyft ridesharing transportation services).

95. *See supra* Section I.B; *see also* Dickinson, *supra* note 51, at 360–72 (detailing the shifts in internet technology that have undermined Section 230).

III. THE INTERNET IMMUNITY ESCAPE HATCH

Despite widespread dissatisfaction with the current internet immunity regime,[96] Congress has thus far made little progress toward change. The polarized political climate makes Section 230 reform feel like a zero-sum game, where to compromise is to lose.[97] And even where agreement might be possible, drafting legislation poses a special challenge because quickly evolving internet communications technologies force legislators to craft abstract legislation to govern an unseen future.[98]

But, by now, political stalemate and rapid technological change have become regular obstacles to governance,[99] for which familiar solutions are available—most commonly, congressional delegation of regulatory authority to an administrative agency.[100] This Part explores the political and practical feasibility of administrative governance in this area, and concludes that an administrative solution would suit the problem but that congressional action to authorize rulemaking is unlikely in the short term, and ultimately proposes a second-best, interim approach: that the current text of Section 230 be leveraged for reform through judicial reinterpretation of the statute's outdated, but helpfully sparse, immunity provisions.

A. Delegation and Compromise

The most common solution to the problems of congressional deadlock and technological change is for Congress to delegate its policy-making authority to an administrative agency. This approach offers several advantages over the traditional legislative process that make it an attractive option for internet immunity

96. *See supra* Sections I.B, II.A.

97. *See supra* Section II.B.1.

98. *See supra* Sections II.B.2–3.

99. *See* Freeman, *supra* note 92, at 2–3, 17–18 (discussing how ideological polarization impedes Congress's ability and willingness to respond to emerging technological developments); William N. Eskridge, Jr., *Vetogates, Chevron, Preemption*, 83 NOTRE DAME L. REV. 1441, 1444–49 (2008) (explaining that, in addition to the Constitution's bicameralism and presentment requirements, House and Senate procedural rules create numerous "vetogates" at which opponents of legislation can kill a bill and that "[t]he obvious consequence of the vetogates structure is that federal statutes are hard to enact").

100. *See generally* Robert L. Rabin, *Federal Regulation in Historical Perspective*, 38 STAN. L. REV. 1189 (1986); David Epstein & Sharyn O'Halloran, *The Nondelegation Doctrine and the Separation of Powers: A Political Science Approach*, 20 CARDOZO L. REV. 947 (1999); Eric A. Posner & Adrian Vermeule, *Interring the Nondelegation Doctrine*, 69 U. CHI. L. REV. 1721 (2002).

reform. First, delegating authority to an administrative agency allows the law to evolve in response to changing circumstances.[101] Congress can enact broad directives authorizing administrative rulemaking and then rely on the agency to handle whatever more detailed regulations and policy making are required. The advantage is this: unlike legislation, administrative delegation requires only that Congress muster a majority sufficient to legislate at one single point in time. If Congress can overcome the constitutional and procedural barriers to legislation even one time, and enact a broad legislative skeleton, that skeleton can then be fleshed out and updated by successive generations of future regulators, even at times when Congress itself could not form a sufficiently powerful majority to legislate.

Delegation also allows Congress to take advantage of agencies' expertise.[102] Legislators tend to be well-educated, with 94% of House Members and 100% of Senators in the current Congress holding at least a bachelor's degree, but far fewer hold advanced degrees.[103] Of those who do, the majority are lawyers, not experts in any field of technical or scientific knowledge.[104] As society becomes more complex and technical, so too do its laws. Although legislators are broadly educated and responsive to their constituents' priorities and viewpoints, they may not have the specialized knowledge, or the time, to design the detailed regulatory structures on which modern society depends. By legislating broad policy goals and assigning the task of detailed

101. *See* Eskridge, *supra* note 99, at 1453–55 (observing that the numerous vetogates impeding legislative change make it difficult to repeal or modify statutes, that "statutes [legislators] enact have got to last a long time—often indefinitely[,]" and that agency delegations provide a mechanism for adapting law to new circumstances).

102. *See* Cass R. Sunstein, *The Most Knowledgeable Branch*, 164 U. PA. L. REV. 1607, 1617 (2016); David B. Spence & Frank Cross, *A Public Choice Case for the Administrative State*, 89 GEO. L.J. 97 (2000); David Epstein & Sharyn O'Halloran, *The Nondelegation Doctrine and the Separation of Powers: A Political Science Approach*, 20 CARDOZO L. REV. 947, 962 (1999); Cass R. Sunstein, *Constitutionalism After the New Deal*, 101 HARV. L. REV. 421 (1987); *see also* Barry Sullivan & Christine Kexel Chabot, *The Science of Administrative Change*, 52 CONN. L. REV. 1 (2020) (discussing administrative expertise as a traditional rationale for delegation and reviewing literature raising objections to reliance on such expertise as a justification for the full breadth of the modern administrative state); Christopher J. Walker, *Legislating in the Shadows*, 165 U. PA. L. REV. 1377, 1406 (2017) (identifying agency expertise as "one of the bedrock rationales" for congressional delegation to agencies and its relationship to agencies' drafting assistance to Congress).

103. *Membership of the 117th Congress: A Profile*, CONG. RSCH. SERV. (Feb. 22, 2022), https://crsreports.congress.gov/product/pdf/R/R46705.

104. *See id.*

rulemaking to administrative experts, both Congress and agencies work within their relative strengths.

Finally, delegation to an agency for rulemaking makes congressional compromise easier. Sometimes competing factions in Congress agree on broad principles—for example, "to protect the public health"[105]—but are unable to agree on a specific legislative strategy to accomplish those goals. In such instances, agency delegation offers an attractive avenue for compromise: Congress can enact legislation that affirms a set of core, agreed-upon policy goals; leave intentionally unresolved the particulars on which Congress was unable to agree; and delegate the responsibility for specific rulemaking on unsettled matters to an administrative agency.[106] By shifting rulemaking on controversial matters to agency decision makers, Congress not only sidesteps the time-consuming (or impossible) give-and-take process of legislative compromise, but it is also insulates itself from any political fallout.[107] Should whatever regulatory structure emerges prove unpopular, Congress can just blame the agency.[108]

105. *See* Clean Air Act, 42 U.S.C. § 7409(b)(1) (authorizing the Environmental Protection Agency to set such national air quality standards as are "requisite to protect the public health"); *see also* Whitman v. Am. Trucking Ass'ns, 531 U.S. 457, 472–76 (2001) (holding that the statutory directive contained a sufficiently intelligible principle and rejecting challenge that regulations issued pursuant to the directive were invalid for improper delegation of legislative authority by Congress).

106. *See* Nathan Alexander Sales & Jonathan H. Adler, *The Rest Is Silence: Chevron Deference, Agency Jurisdiction, and Statutory Silences*, 2009 U. ILL. L. REV. 1497, 1542–43 (2009) (explaining that in the interest of compromise, interest groups and sympathetic legislators leave some issues undecided and delegate their resolution to agencies); Jonathan R. Macey & Geoffrey P. Miller, *The Canons of Statutory Construction and Judicial Preferences*, 45 VAND. L. REV. 647, 666–67 (1992) (observing that statutes have become increasingly complex, that congressional consensus has become more difficult to achieve, and that to find compromise, "[c]ongress has adopted . . . the strategy of passing increasingly broad and amorphous enabling legislation that delegates controversial matters to administrative agencies"); *see also* Frank H. Easterbrook, *Statutes' Domains*, 50 U. CHI. L. REV. 533, 540 (1983) ("Almost all statutes are compromises, and the cornerstone of many a compromise is the decision, usually unexpressed, to leave certain issues unresolved.").

107. *See* Nicholas Almendares, *Blame-Shifting, Judicial Review, and Public Welfare*, 27 J.L. & POL. 239 (2012) (discussing the blame-shifting phenomenon and defending its usefulness against the criticism that delegation may encourage Congress to act contrary to the public interest); Lisa Schultz Bressman, *Chevron's Mistake*, 58 DUKE L.J. 549, 568 (2009) (noting that delegation allows congress to avoid blame for controversial choices while also claiming credit for taking broad action to address the problem); Macey & Miller, *supra* note 106, at 666; *see also* Kenneth A. Shepsle, *The Strategy of Ambiguity: Uncertainty and Electoral Competition*, 66 AM. POL. SCI. REV. 555 (1972).

108. Supporters of broad delegation note that although delegation to an agency may partially protect legislators from blame, legislators are still accountable to voters for their

These features point to internet immunity law as an appropriate target for administrative rulemaking. The internet and related technologies are highly complex and notorious for fast-paced change. And although there is agreement among legislators on basic principles—that free expression on the internet should be protected and that online wrongdoing should be punished—they have not been able to agree on a specific legislative approach. Delegation to an administrative agency would seem to be the natural solution. Congress could build a consensus at a high level of generality around a set of core principles, with those legislators most focused on internet wrongdoing ceding ground to those most concerned with free expression, and vice versa, and then draft an enabling statute that identifies and authorizes an agency to pursue those broadly stated policy objectives.

Unfortunately, apt as it may be, even the agency-delegation option does not appear likely to overcome congressional deadlock on the internet-immunity issue. Congress has made no move toward either detailed legislation or a broad-brush enabling statute that would authorize administrative rulemaking. And those numerous bills that have been proposed would tweak existing language, not overhaul the statute. Section 230 is poised to remain the law of the land for some time.

B. The Stopgap Delegation That Already Is

Because internet technology changes rapidly and a congressional majority has been difficult to muster, one solution to the internet immunity question would be for Congress to enact high-level, future-proof legislation at whatever level of generality consensus is possible. It could then rely on agency rulemaking or judicial elaboration to apply Congress's broad statutory directives to particular cases and adapt the law to technological change. As discussed previously, however, congressional deadlock and political polarization have prevented legislative efforts. In the short term, neither legislation to reform Section 230 nor to delegate administrative rulemaking authority is likely. But hope is not lost. As this section will show, even though no fresh legislation from

decision to delegate, and agencies are themselves accountable to the president. *See* Posner & Vermeule, *supra* note 100, at 1721, 1748–50; Cass R. Sunstein, *Nondelegation Canons*, 67 U. CHI. L. REV. 315, 323 (2000). The extent to which delegation insulates legislators from blame for regulator policy choices is a debated question. For a recent discussion of the issue, see David Schoenbrod, *Statutory Junk*, 66 EMORY L.J. ONLINE 2023, 2029 (2017).

Congress is forthcoming, significant reform is possible through an unlikely source: the Section 230 internet immunity statute already on the books.

Forget, for a moment, the decades of judicial precedent that created the internet immunity doctrine that we now know. Instead, look at the simple words adopted by Congress in 1996: "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."[109]

Section 230(c)(1)[110] is famously short—a mere twenty-six words.[111] Adding the rest of subsection (c) brings the count to 132, and even the entire section comes in under 1,000 words, at 981. By contrast, President Trump's May 2020 executive order interpreting subsection (c) is more than double that length.[112] The provision is barely an ink blot compared to behemoth congressional enactments governing other major issues such as atomic energy,[113] interstate transportation,[114] and corporate financial reporting.[115]

Not only is the provision short, but its language addresses internet immunity at an extraordinarily high level of generality—perhaps the only level that would have made sense in 1996, when the virtual world we know today was just coming into existence.[116]

109. 47 U.S.C. § 230(c)(1).

110. Section 230's key provision is subsection (c), paragraph (1), the provision invoked by defendants in almost all internet immunity cases. Paragraph (2) of that subsection provides a specific, "Good Samaritan" defense to entities that voluntarily censor objectionable material against claims that by censoring they assume liability for content not censored. Subsections (a) and (b) identify the background findings and policies that Congress intended the statute to promote, subsection (d) requires internet service providers to notify users that parental controls are commercially available, and subsections (e) and (f) define the statute's terms and interaction with other state and federal laws. *See* 47 U.S.C. § 230.

111. *See* 47 U.S.C. § 230(c). In his "biography" of Section 230, *The Twenty-Six Words That Created the Internet*, Jeff Kosseff memorably recounts how these few, unassuming words tucked into the Communications Decency Act came to govern and, indeed, *create* the modern internet. *See* KOSSEFF, *supra* note 3, at 1–8.

112. *See* Preventing Online Censorship, 85 Fed. Reg. 34,079–83 (May 28, 2020).

113. *See* Atomic Energy Act of 1946, Pub. L. No. 83–703, 68 Stat. 919 (1954) (codified at 42 U.S.C. § 2011 *et seq.*) (43 pages).

114. *See* ICC Termination Act of 1995, Pub. L. No. 104–88, 109 Stat. 803 (codified in scattered sections of 49 U.S.C.) (157 pages).

115. *See* Sarbanes-Oxley Act of 2002, Pub. L. No. 107–204, 116 Stat. 745 (codified in scattered sections of 15, 18, and 28 U.S.C.) (66 pages).

116. *See* Dickinson, *supra* note 51, at 367–72 (discussing the dramatic evolution of the internet in the decades since Section 230 was enacted, particularly its expansion beyond the publication-centric, mass-media-like entities of the 1990s to the complete virtual world that we have today).

The statute applies to any "interactive computer service," which it defines as anything that involves multiple computer users communicating.[117] It makes no distinction between smartphone apps and websites, between online publications and social media sites, between content distributors and sellers of goods and services, or even between internet service providers and the websites whose data they relay. If an entity is online, it is an interactive computer service, and a single rule applies: It may not be held responsible for others' information.[118]

That is it. That one, twenty-six-word rule along with the Section's all-encompassing definitions are the text by which Congress created internet immunity law. How could Congress have packed so much into so little? The answer, of course, is that it did not, at least not directly. Twitter-powered insurrections[119] and Backpage-aided sex trafficking[120] were decades away, and Congress gave them no thought at all. Instead, it legislated its vision for the future internet with broad brushstrokes that, despite their imprecision, ensured the protection of those principles so central to the modern internet. The law promotes freedom of expression by guaranteeing online entities' ability to relay the massive volume of data that flows through systems without incurring liability for others' content.[121] And the law helped to protect a then-nascent internet (and continues to support the

117. More precisely, Section 230 defines "interactive computer service" to mean "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 Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C § 230(f)(2).

118. *See* 47 U.S.C. § 230(c)(1). There are nuances, of course. As mentioned earlier, § 230(c)(2) includes a provision to specifically immunize online entities that make efforts to censor objectionable material to ensure they do not thereby become liable. And § 230(e) enumerates a few specific instances in which online entities are ineligible for immunity, such as violations of intellectual property rights or sex-trafficking laws.

119. *See* Cecilia Kang, *Democrats, In Control, Plan Push Against Tech*, N.Y. TIMES, Jan. 28, 2021, at B1 (describing Democrats' "animus toward digital platforms" as having various motivations, including "that Facebook, Twitter and YouTube allowed President Donald J. Trump and far-right groups to spread disinformation about the election that led to the riot.").

120. *See* John Anderson, *Investigating the Online Enablers of Child Sex-Trafficking*, WASH. POST, May 21, 2017, at E7 (discussing the problem of online sex trafficking via Backpage and industry opposition to efforts to amend Section 230 to exclude sex-trafficking claims).

121. *See* 47 U.S.C. § 230(c)(1) (providing that an "interactive computer service shall [not] be treated as the publisher or speaker of any information provided by another"); *see also id.* at § 230(a) (announcing the finding of Congress that "the Internet . . . "offer[s] a forum for a true diversity of political discourse" and that "[i]ncreasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.").

current vibrant tech industry) by protecting online entities from lawsuits that would hold them responsible for others' actions or for their good-faith attempts to filter harmful or offensive material.[122] The statute affirms those core values on which legislators then and now agree—but at a level of generality that necessarily delegated nuanced elaboration to future decision makers. In short, Section 230 is very much like the enabling statute Congress might enact today.

Section 230's broad language also contains the seeds for reform. Decades of judicial precedent have cemented in place an expansive view of immunity that has spurred calls for change. But the same statutory language could have produced very different results. Postponing, for now, discussion of how decades of judicial precedent could be set aside,[123] the sections that follow show how Section 230's indeterminacy makes it flexible enough to address those areas of internet immunity law that have been the focus of calls for reform: online wrongdoing, disparate treatment of online versus offline entities, content-moderation practices, and perceived censorship bias.

1. Addressing Volitional Wrongdoing

As discussed previously,[124] the courts' prevailing interpretation of Section 230 faces criticism for protecting online wrongdoers. Because the doctrine includes no mental state limitations on immunity, an entity is eligible for immunity even if it is aware of or intends to cause harm.

But this result does not flow necessarily from the text. As Justice Thomas recently explained,[125] looking to the legal backdrop against which Section 230 was enacted points to a different, much narrower

122. *See* 47 U.S.C. § 230(c)(2) (barring liability predicated on "any action voluntarily taken in good faith to restrict access to or availability of material that the [online entity] considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable"); *see also* 47 U.S.C. § 230(a), (b) (announcing findings and policies of Congress that "[t]he rapidly developing array" of online services "represent[s] an extraordinary advance in the availability of educational and informational resources," that such services "have flourished, to the benefit of all Americans," and that "[i]t is the policy of the United States" "to promote the continued development of the Internet" and "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services").

123. This important question is taken up *infra* Section III.C.

124. *See supra* Sections I.B, II.A.

125. *See* Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 14–15 (2020) (Statement of Thomas, J., respecting the denial of certiorari).

understanding of internet immunity. Traditional defamation law distinguishes between *publishers*, like newspapers and book publishers, and *distributors*, like newsstands and bookstores. On one hand, newspapers and other publishers can be liable for defamatory material they print and circulate—even if it is written by third-party authors—because as publishers they promote and exercise editorial control over the material.[126] Mere distributors, like newsstands, on the other hand, generally cannot be liable for defamatory content in the materials they distribute.[127] But this rule is subject to one important exception: a distributor can be held liable for defamation if the distributor knew or had reason to know that the content was defamatory.[128]

Why does any of this matter? Take another look at Section 230. The statute provides that an online entity shall not "be *treated as the publisher* or speaker of any information provided by another . . . ."[129] One plausible alternative[130] interpretation of that

126. *See* Restatement (Second) of Torts § 577 (1977) (stating the general rule regarding publication or republication of defamatory material, under which both the original speaker or publisher and any subsequent party who repeats or republishes the material can be liable); *see also* DAN B. DOBBS ET AL., THE LAW OF TORTS § 520 (2d ed. 2015) (explaining defamation law's broad concept of publication, which means "any communication, by any method, to one or more persons" and naturally includes books and newspapers "if distributed to at least one person besides the plaintiff").

127. *See Malwarebytes*, 141 S. Ct. at 14 (discussing this aspect of pre-internet defamation law in the context of Section 230).

128. *See* Restatement (Second) of Torts § 581 (1977) (providing that "one who only delivers or transmits defamatory matter published by a third person is subject to liability if, but only if, he knows or has reason to know of its defamatory character."); *see also* DOBBS ET AL., *supra* note 126, at § 522 (explaining that in contrast to newspapers, distributors are "essentially a conduit, not an originator or promoter of content" and that "liability cannot be imposed unless the distributor knows or should know of the defamatory content in the materials he distributes").

129. 47 U.S.C. § 230(c)(1) (emphasis added).

130. This is far from the only possible alternative interpretation of the provision. The provision could, for example, be interpreted even more narrowly, as a definitional clause, which would leave in place only § 230(c)(2)'s Good Samaritan immunity. *See* Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir. 2003) (Easterbrook, J.) (proposing this reading in dicta). One important effect of interpreting subsection (c)(1) as a mere definitional clause is that it would leave the scope of publisher and distributor liability as a question of state tort law rather than federal statutory law. Another possibility, initially raised in the Ninth Circuit's influential decision in *Roommates.com*, would narrow immunity by defining content creators to include any website that is even partly "responsible for" content authored by one of its users. *See* Fair Housing Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157, 1166 (9th Cir. 2008). This is an imperfect solution, however, because not all volitional wrongdoing on the internet is related to content authorship. *See* Dickinson, *supra* note 51, at 120–32. Also, despite the theoretical scope of this interpretation, courts after *Roommates.com* have continued to apply immunity broadly, requiring plaintiffs to show an entity's material

language[131] would read as (1) a determination by Congress that internet service providers and other online entities who do not author content are mere distributors, not publishers; [132] and (2) an affirmation of the common-law rule that bars defamation actions against mere conduits, that is, distributors, unless they have actual or constructive knowledge of the unlawful material.[133]

Interpreted this way, the statute could account for some of the concerns that are animating the push for Section 230 reform. The law would continue to protect internet service providers and platforms that unknowingly transmit or host unlawful third-party content (think Verizon, Google Cloud Storage, and Facebook), but would allow claims to proceed against entities like Backpage[134] that intentionally or knowingly host unlawful material. Merely

contribution by "specifically encourag[ing] development of what is offensive about the content" before an entity can be found to have created or developed content. FTC v. Accusearch Inc., 570 F.3d 1187, 1199 (10th Cir. 2009); *see Malwarebytes*, 141 S. Ct. at 16 (Statement of Thomas, J., respecting the denial of certiorari) (noting that courts have narrowly construed content creation "to cover only substantial or material edits and additions").

131. The leading interpretation of § 230(c)(1) is, of course, that of *Zeran v. America Online*, which rejected any distinction between publisher and distributor liability on two grounds. First, *Zeran* noted that a contrary holding would risk indirect censorship of internet users' speech via the heckler's veto. Second, *Zeran* reasoned that because it requires an underlying defamation claim, of which publication is a necessary element, distributor liability is merely a subset of publisher liability, and Section 230's reference treatment of online entities as "publishers" should not be read as distinct from treatment of them as "distributors." *See* 129 F.3d 327, 331–33 (4th Cir. 1997).

132. This interpretation is even more plausible when one considers the circumstances surrounding its enactment. When Congress enacted Section 230, it had firmly in mind the then-recent decision *Stratton Oakmont, Inc. v. Prodigy Services Co.*, in which a New York state trial court held an internet service provider liable for defamatory content posted by a third party on one of the service's message boards. *See* No. 031063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). *Stratton Oakmont* had reasoned that because Prodigy took steps to review and screen offensive content, it had taken on the role of a newspaper-like publisher rather than a mere distributor and could therefore be held liable for repeating the defamer's words. Section 230 rejects that result. *See* H.R. REP. NO. 104-458, at 194 ("One of the specific purposes of this section is to overrule *Stratton-Oakmont v. Prodigy* . . . .").

133. *See Malwarebytes*, 141 S. Ct. at 14–15 (after discussing historical defamation law, concluding this to be the "face value" interpretation of Section 230); Doe v. Am. Online, Inc., 783 So. 2d 1010, 1019–28 (Fla. 2001) (Lewis, J., dissenting) (urging this interpretation while dissenting from the 4–3 majority in an early Section 230 decision); *see also* JOHN C.P. GOLDBERG & BENJAMIN C. ZIPURSKY, RECOGNIZING WRONGS 319–39 (2020) (adopting a similar interpretation of Section 230(c) after analyzing Section 230's interaction with pre-internet defamation law, common law rules regarding voluntary bystander invention, and state law initiatives to enact Good Samaritan statutes designed to protect intervenors from tort liability).

134. *See supra* Section I.B (discussing the allegations against *Backpage* and the First Circuit's decision granting Section 230 immunity).

adopting a different interpretation of Section 230, rather than enacting any new statutory language at all, could accomplish many of the objectives of the EARN IT Act,[135] the See Something, Say Something Act,[136] the Department of Justice's proposed Section 230 reforms,[137] and other proposed reforms targeted to address intentional or knowing facilitation of internet wrongdoing.[138]

There is, of course, a reason early courts interpreted Section 230 differently. Led by the Fourth Circuit's now-famous decision in *Zeran v. America Online*,[139] courts around the country were concerned that free expression would suffer unless they granted broad Section 230 immunity, even to entities with actual knowledge of unlawful content. They feared what is known as the heckler's veto problem: If platforms become liable for any content they are made aware of but fail to take down, platforms might decide to automatically take down, without investigation, any content simply reported to them as objectionable to avoid the cost of investigating.[140] An internet user's post might be taken down and her freedom to speak her mind undermined by the unverified complaint of an internet "heckler." To avoid this problem and thereby further a policy of "freedom of speech in the new and burgeoning Internet medium," early courts granted broad immunity under Section 230 to any claim implicating an entity's "exercise of a publisher's traditional editorial functions—such as

135. Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020, S.3398, 116th Cong. (2020).

136. See Something, Say Something Online Act of 2020, S.4758, 116th Cong. (2020).

137. DOJ SECTION 230 RECOMMENDATIONS, *supra* note 53, at 14–18.

138. *See supra* Section II.A (discussing these and other proposed reforms).

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

140. *See generally* Brett G. Johnson, *The Heckler's Veto: Using First Amendment Theory and Jurisprudence to Understand Current Audience Reactions Against Controversial Speech*, 21 COMM. L. & POL'Y 175 (2016) (discussing the concept of the heckler's veto, whereby an individual is able to restrict another's freedom to speak by filing complaints against, shouting down, heckling, threatening, or otherwise harassing the speaker); *see also* Reno v. ACLU, 521 U.S. 844, 880 (1997) (invalidating portions of the Communications Decency Act, because, among other reasons, the requirement not to communicate indecent speech to "specific persons" "would confer broad powers of censorship, in the form of a 'heckler's veto,' upon any opponent of indecent speech"); Rory Lancman, *Protecting Speech from Private Abridgement: Introducing the Tort of Suppression*, 25 SW. U. L. REV. 223, 253–55 (1996) (discussing the origin of the "heckler's veto" concept).

deciding whether to publish, withdraw, postpone or alter content" even when that entity is made aware that the content is unlawful.[141]

This is a very real concern. Changes to internet immunity doctrine could have significant consequences for the tech industry and free expression online. Narrowing Section 230 immunity would expose online entities to increased legal risk and could undermine free expression by driving entities to curtail third-party speech on their platforms or even eliminate it altogether. Compliance costs and litigation expenses could bog down the tech industry and even threaten the United States' long-standing position as a worldwide technology leader.

Any reform to Section 230 must be undertaken cautiously, and solutions must be carefully tailored to avoid undermining the broader goals of the statute. In another article I present my own preferred (and extremely narrow) proposal for internet immunity reform.[142] Here my aim is different. Rather than press for any particular approach, this Article engages in a thought experiment to explore how broad reform may be possible even within the confines of the existing statute.

Interpreting Section 230(c)(1) afresh, courts could, for example, interpret the provision to bar only claims against unknowing hosting or transmission of unlawful content and to permit claims predicated on knowledge or intent. Subsequent judicial elaboration could then balance the numerous competing concerns that underlie the reform debate, such as victims' interest in civil recourse, the public's interest in robust online discourse and protection from the heckler's veto, and the tech industry's concern that the law not impose on it burdensome litigation costs or an unreasonable obligation to review user complaints regarding content. Courts might decide, for example, that entities with knowledge are not immune, but that an entity's receipt of one complaint in a sea of other complaints is not sufficient to confer actual or constructive knowledge. Or that true knowledge of unlawful material only occurs once a content author concedes the content to be unlawful. Or when the platform admits content's unlawfulness and undertakes to remove it. The possibilities seem endless, and that is

141. *Zeran*, 129 F.3d at 330, 333 (reasoning that even "liability upon notice reinforces service providers' incentives to restrict speech" because the entity would be required to review and investigate so many complaints as to "create an impossible burden").

142. *See* Dickinson, *supra* note 51.

the point. Section 230—as it already exists—is sufficiently flexible to serve as the mechanism for reform.

2. Disparate Treatment of Online and Offline Entities

Another problem with current internet immunity doctrine is its application outside the publication context, which has created a disparity in the law's treatment of online and offline entities. Although Section 230 is publication-centric—it encourages censorship and it speaks in terms of "publishers or speakers" and "content providers"—publication has never been the internet's exclusive function, and it is even less so now than it was in 1996.[143] The internet operates as a virtual world, complete with all manner of goods and services and every kind of wrongdoing. That includes not only publication-related wrongs, like defamation, but also physical-world wrongs, like designing defective smartphone apps or engaging in false advertising or unfair competition.[144]

When online entities engage in these types of wrongdoing, claims asserted against them raise categorically different issues than Section 230 or the internet immunity doctrine it inspired are designed to handle. Rather than argue that an online entity should be responsible for failing to review or moderate third-party content, such claims are analogous to physical-world product defect,[145]

143. *See* Dickinson, *supra* note 51, at 114–25.

144. *See supra* Section I.B (discussing these and other examples).

145. *See, e.g.*, Lemmon v. Snap, Inc., 440 F. Supp. 3d 1103 (C.D. Cal. 2020) (analyzing a negligence claim against Snapchat for alleged defects in design of the speed filter feature of its app, which plaintiff alleged contributed to auto accidents). A Georgia state trial court held similarly in *Maynard v. McGee*, No. 16-SV-89, 2017 WL 384288, at *3 (Ga. State Ct. Jan. 20, 2017) (finding Snapchat immune under Section 230, reasoning that the Snapchat user, not Snapchat, created the content at issue). *But see* Maynard v. Snapchat, Inc., 816 S.E.2d 77, 79–82 (Ga. Ct. App. 2018) (reversing the lower court and declining to extend immunity on grounds that the case did not depend on publication of third-party content); Maynard v. Snapchat, Inc., No. A20A1218, 2020 WL 6375424, at *3–4 (Ga. Ct. App. Oct. 30, 2020) (following failed Section 230 defense and remand, affirming dismissal for lack of duty of product manufacturer to protect against third-party misuses of product).

negligence,[146] or unfair competition claims.[147] They argue that an online entity should have designed its app or website differently, typically to include more safety features, or that it engaged in anticompetitive business practices.

Despite the diversity of online wrongdoing, however, current internet immunity doctrine is still predicated on a bright-line rule designed for the more publication-centric internet of 1996: Content creators may be sued, but online entities that use that content are immune. This content-authorship-based test for immunity becomes problematic in cases where a plaintiff's injury is causally connected to third-party-created content, but the defendant's alleged wrongdoing is not based on a failure to moderate that content.[148] Even for claims related to product defects or unfair competition that do not allege a failure to review third-party content—and thus do not implicate the moderation burden and heckler's veto concern—courts often grant immunity to defendants on the ground that to do otherwise would interfere with the entity's control over "traditional editorial functions."[149] This expansive

146. *See, e.g.*, Daniel v. Armslist, LLC, 926 N.W.2d 710, 716 (Wis. 2019) (analyzing negligence, public nuisance, wrongful death, aiding and abetting tortious conduct, and other claims against Armslist, alleging that it intentionally designed its website to facilitate illegal gun sales); Doe v. Backpage.com, LLC, 817 F.3d 12, 20 (1st Cir. 2016) (analyzing a statutory sex-trafficking conspiracy claim against *Backpage* based on actions the site allegedly took to impede law enforcement efforts, such as email anonymization and stripping metadata from photographs), *cert. denied*, 137 S. Ct. 622 (2017), *superseded by statute*, Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), Pub. L. 115-164, 132 Stat. 1253, *as recognized in* Teatotaller, LLC v. Facebook, Inc., 242 A.3d 814, 820 (N.H. 2020).

147. *See, e.g.*, Caraccioli v. Facebook, Inc., 700 F. App'x 588, 590 (9th Cir. 2017) (affirming dismissal of unfair competition claim alleging Facebook violated its own terms of service to the plaintiff's detriment by failing to block obscene videos of the plaintiff posted to the service by an unknown person); Marshall's Locksmith Service Inc. v. Google, LLC, 925 F.3d 1263, 1265–66, 1272 (D.C. Cir. 2019) (affirming dismissal of the Lanham Act false advertising claims of locksmith companies, which alleged that Google and other online advertising platforms had "conspired to 'flood the market' of online search results with information about so-called 'scam' locksmiths, in order to extract additional advertising revenue" from truly local locksmiths).

148. *See* Dickinson, *supra* note 51 at 125–34 (elaborating on this point and discussing its impact on claims involving volitional wrongdoing, online marketplaces, and defective products).

149. Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997); *see* Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 16–18 (2020) (discussing the breadth of protection over entities editorial decisions and courts' application of immunity in nonpublication contexts). Courts have applied *Zeran*'s protection of "traditional editorial functions" even though applying the doctrine to bar product-defect and other nonpublication claims is in tension with Section 230's publication focus and the logic of *Zeran*

application of Section 230 immunity creates a rift between the law applicable to online versus offline entities by barring some victims from seeking recovery merely because the defendant happens to operate online.[150]

Of course, when it comes to dissemination of online content, that is exactly what Congress intended—to insulate the burgeoning world of internet media from overburdensome regulation.[151] But disparate treatment has cropped up even outside the information-distribution context. Courts have interpreted Section 230 to act as a broad defense to any cause of action at all—whether it be defamation, negligence, housing discrimination, unfair competition, securities fraud, or anything else—in which the defendant's dissemination of third-party-created content is even tangentially related to the plaintiff's injury.[152] Application of Section 230 immunity to all actions, even outside the publication context, has created dissonance between the law of online and

itself, which premised protection of editorial functions despite a culpable mental state on the need to avoid the heckler's veto.

150. *See supra* Section I.B; *see also* Dickinson, *supra* note 51, at 114–34.

151. *See* 47 U.S.C. § 230(b) (expressing the "policy of the United States" to "promote the continued development of the Internet . . . and other interactive media" and "preserve the vibrant and competitive free market that presently exists for the Internet . . . unfettered by Federal or State regulation").

152. *See* Doe v. Backpage.com, LLC, 817 F.3d 12, 19 (1st Cir. 2016) (noting that "[t]he broad construction accorded to section 230 as a whole has resulted in a capacious conception of what it means to treat a website operator as [a] publisher or speaker" and that Section 230 has accordingly been applied to "a wide variety of causes of action, including housing discrimination, negligence, and securities fraud and cyberstalking") (citations omitted), *cert. denied*, 137 S. Ct. 622 (2017), *superseded by statute*, Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), Pub. L. 115-164, 132 Stat. 1253, *as recognized in* Teatotaller, LLC v. Facebook, Inc., 242 A.3d 814, 820 (N.H. 2020); Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1101–02 (9th Cir. 2009) ("[W]hat matters is not the name of the cause of action—defamation versus negligence versus intentional infliction of emotional distress—what matters is whether the cause of action inherently requires the court to treat the defendant as the 'publisher or speaker' . . . . To put it another way, courts must ask whether the duty that the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a 'publisher or speaker.' If it does, section 230(c)(1) precludes liability."). *But see* Doe v. Internet Brands, Inc., 824 F.3d 846, 853 (9th Cir. 2016) (allowing a failure to warn claim to proceed over the assertion of Section 230 defense because although plaintiff's publication of her online profile on the Model Mayhem website was part of the string of causation that led to her sexual assault, the plaintiff's claim that the website failed to warn her about sexual predators on the site did not seek to hold website liable as the publisher or speaker); City of Chicago v. StubHub!, Inc., 624 F.3d 363, 366 (7th Cir. 2010) (Section 230 "does not create an 'immunity' of any kind. It limits who may be called the publisher of information that appears online. That might matter to liability for defamation, obscenity, or copyright infringement. But Chicago's amusement tax does not depend on who 'publishes' any information or is a 'speaker.' Section 230(c) is irrelevant.") (citation omitted).

offline entities. That is because, with one important exception,[153] Section 230 is not a major deviation from the common-law defamation principles that apply to physical-world entities; it does not create a rift in defamation liability for online and offline publishers.[154] Section 230 does, however, mark a major departure from prior law when it is applied to nonpublication claims. Historically, non-authorship of content was not a defense to non-publication claims such as product liability or unfair competition claims. By giving online entities, but not offline entities, a new defense to nonpublication claims, Section 230 created a rift between online and offline entities.

As with volitional wrongdoing,[155] however, the statutory text is amenable to a different reading. Section 230(c)(1) provides that no "interactive computer service shall be *treated as the publisher or speaker* of any information provided by [a third party]."[156] Although historically it has been read broadly, this language could be read much more narrowly, to apply only to publication-related claims like defamation.[157] Indeed, a few courts have done exactly that and declined to apply Section 230 to causes of action for which publication is not a required element.[158] Agency rulemaking or

153. The exception is the treatment under Section 230 of entities with actual or constructive knowledge of defamatory content. Print media entities subject to common-law defamation rules are subject to liability for content they know or should know to be defamatory, whereas under the prevailing interpretation of § 230(c)(1), online entities are immune regardless of knowledge. *See supra* Section II.B.1.

154. *See* RESTATEMENT (SECOND) OF TORTS § 581 cmt. f (1965) ("One who . . . transmits a written message for another is not liable for the defamatory character of the message unless he knows or has reason to know that the message is libelous."); *see also* Brent Skorup & Jennifer Huddleston, *The Erosion of Publisher Liability in American Law, Section 230, and the Future of Online Curation*, 72 OKLA. L. REV. 635, 638–46 (2020) (detailing the evolution of defamation liability for publishers and distributers in the twentieth century from strict liability to a fault-based regime which includes a conduit liability defense and requires knowledge or recklessness because of the impossible burden of moderating mass media).

155. *See supra* Section III.B.1.

156. 47 U.S.C. § 230(c)(1) (emphasis added).

157. It could even be read as a definitional clause that creates no immunity at all and instead merely gives context to § 230(c)(2)'s Good Samaritan immunity provision. *See* Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir. 2003) (proposing this reading in dicta); *see also* Shlomo Klapper, *Section 230 Textualism*, 70 BUFF. L. REV. (forthcoming 2022) (defending this interpretation on textualist grounds). *But see* Chicago Lawyers' Comm. for C.R. Under L., Inc. v. Craigslist, Inc., 519 F.3d 666, 670 (7th Cir. 2008) (Easterbrook, J.) (declining to adopt this reading when presented with the opportunity to do so).

158. *See, e.g.*, City of Chicago v. StubHub!, Inc., 624 F.3d 363, 366 (7th Cir. 2010) (reasoning that Section 230 "limits who may be called the publisher of information that appears online," which "might matter to liability for defamation, obscenity, or copyright

judicial elaboration interpreting Section 230 to apply only to publication-related actions would eliminate the disparity in treatment between online and offline entities.

However, identifying those claims related enough to publication to warrant immunity could prove difficult. Creative plaintiffs would attempt to plead around Section 230 by dressing up what is really a defamation claim as something different. For example, a plaintiff might claim that a defendant platform acted negligently by failing to identify and remove repeat posters of unlawful content from its platform.[159] Or that it tortiously interfered with a contract or prospective business relationship by failing to remove untruthful statements about the plaintiff.[160] Or that it became part of a cyberbullying conspiracy when it failed to intervene despite notice from concerned parents.[161] Courts would need to develop detailed rules to prevent creative lawyers from pleading around the Section 230 defense.

A superior approach, in my view, would be to interpret Section 230(c)(1)'s reference to actions that treat online entities as a

infringement" but not "Chicago's amusement tax"); Airbnb, Inc. v. City & Cnty. of San Francisco, 217 F. Supp. 3d 1066, 1072 (N.D. Cal. 2016) (concluding that Section 230 did not preempt city ordinance that criminalized Airbnb's collection of fees for providing booking services for unregistered short-term residential rental units). Given courts' broad conception of what editorial functions Section 230 protects, however, this requirement is almost always satisfied. *See* Doe v. Backpage.com, LLC, 817 F.3d 12, 19 (1st Cir. 2016) (noting that "[t]he broad construction accorded to section 230 as a whole has resulted in a capacious conception of what it means to treat a website operator as [a] publisher or speaker" and that Section 230 has accordingly been applied to "a wide variety of causes of action, including housing discrimination, negligence, and securities fraud and cyberstalking") (citations omitted), *cert. denied*, 137 S. Ct. 622 (2017), *superseded by statute*, Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), Pub. L. 115-164, 132 Stat. 1253, *as recognized in* Teatotaller, LLC v. Facebook, Inc., 242 A.3d 814, 820 (N.H. 2020). *But see* Doe v. Internet Brands, Inc., 824 F.3d 846, 853 (9th Cir. 2016) (allowing failure to warn claim to proceed).

159. *Cf., e.g.*, Doe v. Twitter, Inc., No. 21-cv-00485-JCS, 2021 WL 3675207, at *32 (N.D. Cal. 2021) (negligence claims against Twitter for failing to remove unlawful videos after notice); Nunes v. Twitter, Inc., 105 Va. Cir. 230 (Va. Cir. Ct. 2020) (plaintiff alleging Twitter liable for negligence "for allowing the defamatory content to remain on [its] internet platform").

160. *See, e.g.*, Whitney Info. Network, Inc. v. Verio, Inc., No. 2:04CV462FTM29SPC, 2006 WL 66724, at *2 (M.D. Fla. Jan. 11, 2006) (alleging tortious interference with business relationship where web host failed to take down website); *see also* Page v. Oath Inc., No. 79, 2022 WL 164008, at *3 & n.31 (Del. 2022) (discussing plaintiff's claim before the trial court, but not pursued on appeal, that defendants tortiously interfered with prospective business relationships by hosting allegedly defamatory articles on their websites).

161. *Cf., e.g.*, Gonzalez v. Google LLC, 2 F.4th 871, 907 (9th Cir. 2021) (conspiracy claim against online platforms under Anti-Terrorism Act for providing material support to terrorist organization); Force v. Facebook, Inc., 934 F.3d 53, 72 (2d Cir. 2019) (same).

"publisher or speaker"[162] of third-party content to mean those actions that would impose on entities a duty to review and moderate third-party-created content.[163] Like limiting Section 230 to publication-related claims, this approach would align the law's treatment of online and offline entities by allowing claims to proceed unless they implicate the content-moderation burden that Section 230 was designed to shield against. But because the definition would focus on the effects claims have on entities rather than the claims' names or elements, the boundary would be easier for rule makers to define.

3. Encouraging Content Moderation

Section 230 has also faced criticism for protecting online platforms that disseminate harmful or offensive material. The prevailing view interprets the statute to immunize online entities against any claim related to "information provided by [a third party]."[164] The defense applies no matter the type of information at issue, be it hate speech, election misinformation, revenge porn, cyber bullying, or anything else.[165] And an entity is eligible for immunity even if it *knows* the content is on its platform and still fails to remove it.[166]

Again, however, the statute could be read very differently. Recall the discussion earlier regarding the pre–Section 230 common

162. 47 U.S.C. § 230(c)(1).

163. *See generally* Dickinson, *supra* note 51, at 134–51 (proposing congressional amendment to Section 230(c)(1) that would produce the same result).

164. 47 U.S.C. § 230(c)(1).

165. *See supra* Section I.B.

166. *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 330, 333 (4th Cir. 1997) (interpreting Section 230 to bar even "liability upon notice"); *see also* Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 15 (2020) (explaining that courts have interpreted Section 230 to confer immunity "even when a company distributes content that it *knows* is illegal"); Doe v. Backpage.com, LLC, 817 F.3d 12, 21–24 (1st Cir. 2016) (dismissing claim despite allegations website acted deliberately because "[w]hatever Backpage's motivations, those motivations do not alter the fact that the complaint premises liability on . . . third-party content"), *cert. denied*, 137 S. Ct. 622 (2017), *superseded by statute*, Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), Pub. L. 115-164, 132 Stat. 1253, *as recognized in* Teatotaller, LLC v. Facebook, Inc., 242 A.3d 814, 820 (N.H. 2020); Barnes v. Yahoo, 570 F.3d 1096, 1098–103 (9th Cir. 2009) (dismissing negligence claim where defendant Yahoo acknowledged nude photos posted of plaintiff without her consent but promised to follow through on its promise to remove them); Doe v. Am. Online, Inc., 783 So. 2d 1010, 1018 (Fla. 2001) (dismissing claim where plaintiff alleged AOL was aware that a particular user of its service was transmitting unlawful photographs and yet declined to intervene).

law.[167] Historically, the law distinguished between publishers, like newspapers, and distributors, like newsstands, and held that whereas publishers could always be liable for circulating defamatory third-party speech, distributors could be liable only if they knew or should have known the speech to be defamatory.[168] In light of this historical distinction, one possible interpretation of Section 230(c)(1) is that it designates online entities as distributors, not publishers, thereby protecting them from liability for third-party content they distribute, but only if they do not have knowledge of its unlawfulness.[169]

Judicial elaboration could expand this idea of actual or constructive knowledge beyond its common-law boundaries[170] to include the concept of negligent or willful blindness. For example, knowledge of unlawful content could be defined to include lack of knowledge due to failure to include content-flagging mechanisms by which a platform's users can submit content for review. Or it could include lack of knowledge for failure to timely review and respond to user-flagged content. Knowledge imputation could even be limited to certain categories of material, thereby allowing courts to impose a moderation requirement for only the very most harmful types of content.[171] With Section 230(c)(1) immunity

167. *See supra* Section III.B.1.

168. *See* RESTATEMENT (SECOND) OF TORTS § 581 (1977) (providing that "one who only delivers or transmits defamatory matter published by a third person is subject to liability if, but only if, he knows or has reason to know of its defamatory character").

169. *See supra* Section III.B.1.

170. *See* RESTATEMENT (SECOND) OF TORTS § 12 (1965) (explaining that as used in the Restatement, "reason to know" denotes "the fact that the actor has information from which a person of reasonable intelligence or of the superior intelligence of the actor would infer that the fact in question exists, or that such person would govern his conduct upon the assumption that such fact exists"); *see also Knowledge*, BLACK'S LAW DICTIONARY (11th ed. 2019) (defining constructive knowledge as "[k]nowledge that one using reasonable care or diligence should have, and therefore that is attributed by law to a given person").

171. Whether aimed at curtailing online entities' volitional wrongdoing, see *supra* Section II.B.1, or at encouraging more robust content-moderation efforts, judicial exploration of what constitutes sufficient "knowledge" of unlawful content within the meaning of Section 230 to trigger distributor liability would parallel judicial efforts in the context of copyright law to determine what constitutes an online entity's "red flag" awareness of copyright infringement so as to take the entity outside of the Digital Millennium Copyright Act's (DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (codified at 17 U.S.C. §§ 101–1301), safe harbor provisions for online service providers. *See* 17 U.S.C. § 512 (providing safe harbor immunity from copyright infringement claims to online service providers when certain conditions are satisfied, including that they are "not aware of facts or circumstances from which infringing activity is apparent"). In that context, courts have converged around a standard requiring knowledge of specific files or activity, not mere generalized knowledge

narrowed to apply only where an entity lacks knowledge, and knowledge expanded to include failure to adopt sufficiently robust moderation practices, the statute would allow state and federal regulators to adopt rules banning online entities' transmission or hosting of disfavored material, right up to the boundaries of the First Amendment.[172]

Whether any of this is a good idea is a separate question. Indeed, in my view,[173] such changes would do far more harm than good. Exposing online entities to notice-based legal liability would impose an enormous content-moderation burden that would undermine free expression. Platforms could be compelled to heavily censor user speech or disallow online posting altogether to avoid the risk of liability. But the idea of exposing online entities to limited, knowledge-based liability for at least certain types of wrongdoing has proponents in Congress and some public support. The point here, rather than to reiterate my own views of policy, is to show what could be accomplished within the confines of the existing statute. Section 230's effect on content-moderation practices could be dramatically altered with no amendment at all to the statute's text.

4. Preserving Internet Free Expression

Noting that Section 230 was intended, in part, to protect the internet as "a forum for a true diversity of political discourse,"[174] some critics have challenged the availability of internet immunity even to entities whose content-moderation practices may be politically biased or disfavor marginalized voices.[175] As courts have interpreted it, Section 230(c)(1) is available to any online entity as a defense to claims predicated on third-party-created content,

of misuse for infringement, as the level of knowledge that will remove an entity from the protection of DMCA's safe harbor. *See* Capitol Recs., LLC v. Vimeo, LLC, 826 F.3d 78, 93 (2d Cir. 2016); Ventura Content, Ltd. v. Motherless, Inc., 885 F.3d 597, 609–10 (9th Cir. 2018); BWP Media USA, Inc. v. Clarity Digital Group, LLC, 820 F.3d 1175, 1182 (10th Cir. 2016).

172. For a discussion of the different procedural and substantive scope of Section 230 compared to the First Amendment, see Goldman, *supra* note 11, at 36–46.

173. *See* Dickinson, *supra* note 51, at 114–20, 134–51 (discussing the importance of Section 230 to prevent online entities from facing an overwhelming burden to moderate content, the need to protect free expression against collateral censorship, and proposing reforms to Section 230 centered around those goals).

174. 47 U.S.C. § 230(a)(3).

175. *See supra* Sections I.B, II.A.

whether it engages in neutral content moderation, biased content moderation, or no content moderation at all.[176]

This feature of Section 230 doctrine, too, could be reformed by reinterpreting the existing statute.[177] As discussed in the previous section, Section 230(c)(1) could be interpreted to protect online entities from liability for third-party content only where they lack knowledge of the content's unlawfulness.[178] Knowledge could be interpreted to include negligent or willful blindness, including failure to adopt robust content-moderation procedures. Such mandated procedures might include a requirement that platforms publish detailed content-moderation policies to notify the public what types of content they permit.

Next, with all online entities compelled to issue detailed, content-moderation policies, further judicial rulemaking could interpret Section 230's reference to "publisher or speaker" liability[179] not to protect online entities against non-publication claims,[180] including false advertising or breach of contract for failure to abide by their stated moderation policies.[181] This two-step approach would force platforms to carefully articulate their policies and make them available for public inspection and criticism.

176. *See* 47 U.S.C. § 230(c)(1); *see also* Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir. 2003) (observing that Section 230 "makes ISPs indifferent to the content of information they host or transmit: whether they do (subsection (c)(2)) or do not (subsection (c)(1)) take precautions, there is no liability under either state or federal law").

177. The same or similar reforms could also be accomplished by judicial or legislative determination that social-media platforms should be treated as common carriers and required transmit by all users equally, regardless of its viewpoint. *See* Biden v. Knight First Amendment Institute at Columbia Univ., 141 S. Ct. 1220, 1221 (2021) (Thomas, J. concurring in denial of petition as moot) (suggesting that given social-media platforms' market dominance and prominent role in modern discourse perhaps they should be treated as common carriers). *But see* Gregory M. Dickinson, *Big Tech's Tightening Grip on Internet Speech*, 54 IND. L. REV. (forthcoming 2022) (suggesting competitive market forces be given more time to operate before any such drastic intervention).

178. *See supra* Section III.B.3.

179. 47 U.S.C. § 230(c)(1).

180. *See supra* Section II.B.2.

181. Current internet immunity doctrine bars such claims. *See* Marshall's Locksmith Serv., Inc. v. Google, LLC, 925 F.3d 1263, 1265–66, 1272 (D.C. Cir. 2019) (affirming dismissal of locksmith companies' false advertising claims, which alleged that Google and other online advertising platforms had "conspired to 'flood the market' of online search results with information about so-called 'scam' locksmiths, in order to extract additional advertising revenue" from truly local locksmiths); Caraccioli v. Facebook, Inc., 700 F. App'x 588, 590 (9th Cir. 2017) (affirming dismissal of unfair competition claim alleging Facebook violated its own terms of service to plaintiff's detriment by failing to block obscene videos of plaintiff posted to the service by an unknown person).

Should an entity fail to abide by its stated policies, an aggrieved user would have recourse in the courts by asserting a claim for false advertising or breach of contract.

This is the riskiest proposal of all. Unless courts were to grant online entities significant deference on their moderation decisions, the requirement could pressure online entities to adopt strict, bright-line content moderation policies, increase litigation costs, and press platforms toward heavy-handed censorship to avoid legal liability. The result could very well be *less*, not more, freedom of expression for online speakers. Dangerous as such reforms may be, however, the point of this Article is to demonstrate what is possible. As with other reform proposals, judicial elaboration on the current text could achieve the objectives of the very bills pending in Congress,[182] all without changing a word of Section 230.

C. Parrying Path Dependency

Now it is time to take up the crucial question previously deferred[183]: Who cares if Section 230 *could be* interpreted differently? What really matters is how it *has been* interpreted. Courts adopted an extremely broad approach to immunity in the internet's early days. Does not that precedent now bind us to the status quo? The answer, as this section will explain, is no. Even without new congressional action, Section 230's extreme breadth leaves state and federal courts ample room to break free from the existing body of case law and chart a new course.

The traditional process for statutory reform in the courts is the gradual, common-law-like narrowing and distinguishing of past decisions. However, the extremely broad language of courts' early Section 230 precedents make that approach difficult in this context.[184] The prevailing interpretation, for example, allows for no

182. For discussion of pending proposals, see *supra* Section II.A.

183. *See supra* Section III.B.

184. Several factors contributed to the law's development toward its current state. First, the seminal Section 230 cases were decided in the early years of the internet and, like the statute itself, designed for an online world very different from today's. Smartphones, social media platforms, and even much of the online commercial activity that is now so familiar were still years away, and the early cases necessarily made no distinction between those technologies and the more traditional internet providers and media outlets prevalent on the internet of the 1990s. *See* Dickinson, *supra* note 51, at 367–72 (discussing the internet's evolution from the 1990s to today). Second, courts were concerned to protect the nascent internet from legal liability that could threaten its growth and undermine what was then a burgeoning new medium for free expression. This included protecting them even against

mental-state-based limitation on immunity for entities that have knowledge of unlawful material on their platforms.[185] And the only basis on which the defense permits liability to be imposed is for authorship of content, even though not all internet wrongdoing involves content creation.[186]

The most promising direction for precedential evolution is the small body of case law that has attempted to limit the Section 230 defense to publication-related claims. So limiting Section 230 would allow product liability, unfair competition, negligence, and other claims to proceed, while still protecting online entities from claims related to publication of third-party content.[187] In practice, however, it has been difficult for courts to identify and enforce the border between claims that are sufficiently related to publication to trigger immunity and those that are not. A hard rule barring defamation claims, for example, just presses litigants to recharacterize their claims and plead them as other causes of action. But courts could develop more nuanced tests to catch such plead-arounds, while allowing true nonpublication claims to proceed. For example, as discussed previously,[188] courts might revise the publication-related inquiry[189] to ask whether the plaintiff's theory of relief would require the online entity to review and moderate third-party content to prevent the alleged harm. Regardless of any

claims that alleged actual knowledge of unlawful content. For entities that transmit large quantities of third-party-created content, the threat of notice-based legal liability could push them to heavily censor content rather than undertake the cost and risk of careful pruning. *See supra* Section III.B.1; Gregory M. Dickinson, *Toward Textual Internet Immunity*, 33 STAN. L. & POL'Y REV. 1, 6–7 (2022) (discussing *Zeran* and early courts' concern to protect against the "heckler's veto" problem). Third, this was the approach adopted by *Zeran*, the first federal appellate court to interpret Section 230. The decision was authored by the widely respected Judge J. Harvey Wilkinson III, who provided a thorough analysis of the statute's underlying purposes and concluded that broad immunity would best serve those ends. Given the natural tendency of courts to follow carefully reasoned precedents and to harmonize the law among the federal circuits, other jurisdictions quickly, and largely uncritically, followed the Fourth Circuit's lead. *See* Klapper, *supra* note 157, at Section I (discussing the historical genesis of current Section 230 doctrine).

185. *See supra* Sections I.B, II.A.

186. *See supra* Sections I.B, III.B.1–2.

187. *See, e.g.*, City of Chicago v. StubHub!, Inc., 624 F.3d 363, 366 (7th Cir. 2010) (Easterbrook, J.) (reasoning that Section 230 "limits who may be called the publisher of information that appears online," which "might matter to liability for defamation, obscenity, or copyright infringement" but not "Chicago's amusement tax").

188. *See supra* Section III.2.

189. *See* 47 U.S.C. § 230(c)(1) (protecting online entities against claims that treat them as "publisher or speaker" of third-party-created content).

new test adopted, however, case law evolution of Section 230's publication-related limitation can only go so far.[190] It might align the law's treatment of online and offline entities, and it might partially address volitional wrongdoing, but reforming platforms' content-moderation practices would require a different approach.

For more significant reform, the United States Supreme Court is the obvious candidate. Despite numerous opportunities in recent years,[191] the Court has never issued a decision interpreting Section 230. But that may soon change. Last term the Supreme Court again declined to interpret Section 230 when it denied a request to review the Ninth Circuit's decision in *Malwarebytes v. Enigma*.[192] Although he agreed with his colleagues' decision not to hear the case, Justice Thomas took the unusual step of issuing a statement to explain why, "in an appropriate case," the Supreme Court should take up a Section 230 case to consider the appropriate scope of internet immunity.[193] If the Court were to interpret Section 230, it would be

190. The limited power of lower courts to shape, but not wholly undo, existing Section 230 doctrine is a good thing—a feature of our legal system, not a bug. Were jurisdictions across the country suddenly to adopt radically different approaches from one another to internet intermediary liability, online entities (which often operate in numerous jurisdictions) would face significantly increased legal uncertainty and compliance costs, which they might well pass on to their users. Users of legal services, for their part, would face increased costs for services and uncertainty of their own legal rights. *See* Dickinson, *supra* note 51, at 386–87, 392–94 (discussing the costs to online entities of legal uncertainty and rejecting on that basis a multistate approach to intermediary liability reform).

191. *See, e.g.*, Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019), *cert. denied*, 140 S. Ct. 2761 (2020); Daniel v. Armslist, LLC, 926 N.W.2d 710 (Wis. 2019), *cert. denied*, 140 S. Ct. 562 (2019); Hassell v. Bird, 420 P.3d 776 (Cal. 2018), *cert. denied sub nom*. Hassell v. Yelp, Inc., 139 S. Ct. 940 (2019); Doe v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016), *cert. denied*, 137 S. Ct. 622 (2017), *superseded by statute*, Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), Pub. L. 115-164, 132 Stat. 1253, *as recognized in* Teatotaller, LLC v. Facebook, Inc., 242 A.3d 814, 820 (N.H. 2020).

192. *See* Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13 (2020).

193. *See id.* (Statement of Thomas, J., respecting the denial of certiorari). Other signals also suggest the Supreme Court is considering wading into the internet-law debate. Following *Malwarebytes*, in May 2022, Justice Thomas authored an opinion supporting the Court's denial of certiorari for lack of finality for an action against Facebook by an underage girl trafficked for sex, but again suggesting that consideration of Section 230's scope may be warranted: "As I have explained, the arguments in favor of broad immunity under § 230 rest largely on 'policy and purpose,' not on the statute's plain text. Here, the Texas Supreme Court recognized that '[t]he United States Supreme Court—or better yet, Congress—may soon resolve the burgeoning debate about whether the federal courts have thus far correctly interpreted section 230.' Assuming Congress does not step in to clarify § 230's scope, we should do so in an appropriate case." Doe v. Facebook, Inc., 142 S. Ct. 1087, 1088 (2022) (Statement of Thomas, J. respecting denial of certiorari) (internal citations omitted). Similarly, last year the Court took up *Biden v. Knight First Amendment Institute at Columbia University*, 141 S. Ct. 1220 (2021), a case that challenged former President Trump's decision

writing on a completely blank slate. It could affirm the prevailing interpretation found in existing case law, adjust that case law where it perceives past courts to have gone astray, or completely upend the past cases and take internet immunity doctrine in an entirely new direction, including reforms to platforms' content-moderation practices or any of the other possibilities discussed above.[194]

Another path to reform is through those state high courts around the country that have not yet interpreted Section 230. Because the Supreme Court has never interpreted the statute, the question of its scope has been left for independent resolution in sixty-three jurisdictions—the thirteen federal circuit courts of appeal and the high courts of the fifty states.[195] Thus far, those courts have coalesced around the extremely broad internet immunity doctrine that is now the target of reform efforts. But with

to block certain users from responding to his tweets. The Court ultimately dismissed the challenge as moot after Trump's election loss, but here too Justice Thomas took the opportunity to comment on the legal challenges surrounding online speech and social media sites. *See id.* at 1221 (Thomas, J. concurring). The Supreme Court is rightly cautious when it reshapes laws of such great national significance, often preferring targeted, narrow opinions, but it has shown itself willing to upend even core legal doctrines if it deems them sufficiently misguided or harmful to society. *See, e.g.*, Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021) (interpreting "exceeds authorized access" under Computer Fraud and Abuse Act not to include defendant's use of database for an improper purpose); Nautilus, Inc. v. Biosig Instruments, Inc., 572 U.S. 898, 910 (2014) (rejecting Federal Circuit's test for whether a patent claim is "definite," reasoning that it would create "powerful incentives to inject ambiguity" into claims); Limelight Networks, Inc. v. Akamai Techs., Inc., 572 U.S. 915, 925 (2014) (rejecting Federal Circuit doctrine permitting liability for indirect patent infringement even in the absence of direct infringement).

194. *See supra* Sections III.B.1–4.

195. Although state courts are bound by the Supreme Court on matters of federal law, they are not required to follow decisions of the federal courts of appeal. *Compare* James v. City of Boise, 136 S. Ct. 685, 686 (2016) (per curiam) (reversing Idaho Supreme Court decision that it was not bound to follow the Supreme Court's interpretation of a federal statute and explaining that it is the Supreme "Court's responsibility to say what a federal statute means" and "it is the duty of other courts to respect that understanding"), *with* Owsley v. Peyton, 352 F.2d 804, 805 (5th Cir. 1965) ("Though state courts may for policy reasons follow the decisions of the Court of Appeals whose circuit includes their state, they are not obliged to do so.") (citation omitted). *See also* Lockhart v. Fretwell, 506 U.S. 364, 376 (1993) (Thomas, J., concurring) ("[N]either federal supremacy nor any other principle of federal law requires that a state court's interpretation of federal law give way to a (lower) federal court's interpretation."); Arizonans for Off. English v. Arizona, 520 U.S. 43, 66 n.21 (1997) (noting that "the stare decisis effect of [a federal district] court's ruling was distinctly limited" because it was "not binding on the Arizona state courts"). For an intriguing alternative view that state courts should be bound by lower federal courts' interpretations of federal law, see Amanda Frost, *Inferiority Complex: Should State Courts Follow Lower Federal Court Precedent on the Meaning of Federal Law?*, 68 VAND. L. REV. 53 (2015).

momentum growing for change, those jurisdictions[196] that have not yet interpreted Section 230 could consider alternatives to the prevailing view to address current doctrine's perceived flaws. By doing so, those courts could exert pressure on other courts to reconsider prior decisions or even spur the Supreme Court to action to resolve inconsistencies between jurisdictions.

Finally, recent actions by Congress and the Supreme Court have cast doubt on the prevailing interpretation of Section 230 and in doing so have opened a potential path to reform even for those courts that are precedentially committed to current internet immunity doctrine. In his statement accompanying denial of certiorari in *Malwarebytes*, Justice Thomas lamented that lower courts "have long emphasized nontextual arguments when interpreting § 230, leaving questionable precedent in their wake."[197] In particular, he questioned courts' application of Section 230 immunity in many of the same contexts that have drawn Congress's attention: platforms that leave content on their sites that they know to be unlawful; those that seek out and curate unlawful content for their sites; and claims outside the publishing context, such as those related to defective products.[198] Sensing a gap between Congress's words and current internet immunity doctrine, Justice Thomas urged the Court in a future case to consider whether "the text of [Section 230] aligns with the current state of immunity enjoyed by Internet platforms."[199]

196. The high courts of thirty-four states have never interpreted Section 230: Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, Hawaii, Idaho, Indiana, Kansas, Kentucky, Louisiana, Maine, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Jersey, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, West Virginia, and Wyoming.

197. *Malwarebytes*, 141 S. Ct. at 14.

198. *See id.* at 15–18; *see also supra* Sections I.B–II.A (discussing problems with current internet immunity doctrine and various proposals for reform under consideration by Congress).

199. *Malwarebytes*, 141 S. Ct. at 14.

Congress noted similar concerns when it enacted FOSTA[200] in 2018 in response to the First Circuit's *Backpage.com*[201] decision.[202] With FOSTA, Congress sent a strong message to the nation's courts that they have been misapplying Section 230. In its report recommending that FOSTA be enacted into law, the House Committee on the Judiciary lamented that "[i]n civil litigation, bad-actor websites have been able to successfully invoke [Section 230] despite engaging in actions that go far beyond publisher functions."[203] And throughout the legislative process, representatives from across the political spectrum took the opportunity to criticize the courts' overzealous application of Section 230 immunity. Indeed, when introducing the bill, Senator Portman who coauthored FOSTA and who also voted to enact the Section 230 of the CDA in 1995 explained that although "I believe that the Communications Decency Act is a well-intentioned law that has an important purpose. . . . the law was not intended to protect those who willingly facilitate illegal conduct, such as sex trafficking[.]"[204] When it amended Section 230 to specifically exclude sex-trafficking claims, Congress "clarif[ied] that section

200. Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), Pub. L. 115-164, 132 Stat. 1253 (2018).

201. Doe v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016), *cert. denied*, 137 S. Ct. 622 (2017), *superseded by statute*, Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), Pub. L. 115-164, 132 Stat. 1253, *as recognized in* Teatotaller, LLC v. Facebook, Inc., 242 A.3d 814, 820 (N.H. 2020).

202. *See supra* Sections I.B, III.B.1 (discussing the *Backpage* decision and the FOSTA amendment to Section 230).

203. H.R. REP. NO. 115-572, Part 1, at 4 (2018) (citing *Backpage.com* and apparently disagreeing with that court's conclusion that the plaintiffs' lawsuit treated the site as a publisher or speaker within the meaning of Section 230); *accord* S. REP. NO. 115-199, at 2 (2018) (Section 230's "protections have been held by courts to shield from civil liability . . . nefarious actors, such as the website Backpage.com.").

204. 163 CONG. REC. S4670–71 (daily ed. Aug. 1, 2017) (noting that even though the *Backpage.com* court "found that the victims made a strong case that backpage [sic] tailored its site to make underage sex trafficking easier," it found it immune "no matter how complicit the website was"); *accord* 164 CONG. REC. S1853 (daily ed. Mar. 21, 2018) (statement of Sen. Heitkamp, D-North Dakota, who sponsored FOSTA) ("I never believed that the [CDA] protected [Backpage.com] from . . . civil penalty if they were complicit and, in fact, abetted these crimes. I never believed that, *but there were judges in America who did*.") (emphasis added); 164 CONG. REC. H1277 (daily ed. Feb. 27, 2018) (statement of Rep. Collins, R-Georgia, who supported FOSTA) ("[S]ome websites have successfully invoked the section 230 immunity provision despite engaging in actions that venture far outside the scope of those envisioned by the statute . . . Doe v. Backpage . . . held that . . . this law shielded the company from the claims that were filed by the child victims. . . . FOSTA is a recommitment to Americans that Congress never intended to create a system that allows business to commit crimes online that they could not commit offline.").

230 . . . does not prohibit the enforcement against providers . . . of interactive computer services of . . . civil law relating to . . . sex trafficking"[205] and announced "the sense of Congress that . . . section 230 . . . was never intended to provide legal protection to [such] websites[.]"[206]

FOSTA and Justice Thomas's statement in *Malewarebytes* are signals to the nation's courts that it may be time to revisit long-standing case law on Section 230. The world has changed since courts' early decisions. The internet is now the dominant forum in which Americans voice their political views; it has transformed into a complete virtual world for the sale of goods and services; and it is now populated with all the bad actors and harms of the real world.[207] These developments have broken down the bright-line rules and tidy categories of early cases and forced courts to address a more nuanced world while tied to sweeping precedents that they might decide differently today.[208]

But the courts have the power to change course. State high courts or, less likely, en banc reconsideration by the United States Federal Courts of Appeal could quickly wipe the slate clean and give the judiciary a fresh opportunity to interpret Section 230 in light of the last twenty years of internet history. Courts could add distinctions and nuance to existing bright-line rules to address volitional wrongdoing and disparate treatment of online versus offline entities.[209] Or, taking a bolder approach, they could apply Section 230 to address content-moderation and censorship-bias concerns surrounding online expression.[210] The path to reform is open—no amendment required.

CONCLUSION

Although Section 230 continues to play a critical role regulating internet liability, the law is insufficiently nuanced to govern the broad spectrum of entities that populate the modern internet. Congress is deadlocked and unable to act, but an alternative, perhaps superior, path to reform is available through the very

205. Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (FOSTA), Pub. L. No. 115-164, 132 Stat. 1253.

206. *Id.* at § 2(1).

207. *See* Dickinson, *supra* note 51, at 120–34.

208. *See id.* at 120–25.

209. *See supra* Sections III.B.1–2.

210. *See supra* Sections III.B.3–4.

statute already on the books. Because of its extreme breadth and linguistic indeterminacy, Section 230 acts as a broad delegation of interpretive authority to the judiciary, which now holds the power to achieve the very reforms on which Congress has been unable to act: intentional online wrongdoing, disparate treatment of online versus offline entities, harmful internet content, and biased censorship practices. This Article lays the foundation for courts to press forward with reforms by reading Section 230 afresh, illuminated by the last twenty years of internet history.