

# A USER’S GUIDE TO SECTION 230, AND A LEGISLATOR’S GUIDE TO AMENDING IT (OR NOT)

*Jeff Kosseff*<sup>†</sup>

## ABSTRACT

Section 230 of the Communications Decency Act, which immunizes online service providers from liability for user content, is key to the business models of some of the nation’s largest online platforms. For two decades, the 1996 statute was mostly unknown outside of technology law circles. This has changed in recent years, as large social media companies have played an increasingly central role in American life and have thus faced unprecedented scrutiny for their decisions to allow or remove controversial user content. Section 230 has entered the national spotlight as a topic of national media coverage, congressional hearings, and presidential campaign rallies. Unfortunately, not all this attention has accurately portrayed why Congress passed § 230 or how the statute works. The misunderstandings of the law are particularly troubling as Congress is considering dozens of proposals to amend or repeal it. This Article attempts to set the record straight and provide a “user’s guide” to the statute, along with principles for legislators to consider as they evaluate amendments to this vital law.

## TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION .....</b>	<b>758</b>
<b>II.</b>	<b>WHY CONGRESS PASSED § 230.....</b>	<b>761</b>
	A. LIABILITY FOR DISTRIBUTORS BEFORE § 230 .....	761
	B. WHAT § 230 ACTUALLY SAYS.....	768
<b>III.</b>	<b>HOW § 230 WORKS.....</b>	<b>773</b>
	A. THE BROAD SCOPE OF § 230(C)(1).....	773
	B. WORKING AROUND § 230(C)(1) .....	779
	1. <i>Development or Creation of Content</i> .....	780
	2. <i>Treatment as Publisher or Speaker</i> .....	782
	C. JUDICIAL CALLS FOR § 230 REFORM.....	785
<b>IV.</b>	<b>PRINCIPLES FOR § 230 REFORM .....</b>	<b>788</b>

---

DOI: <https://doi.org/10.15779/Z38VT1GQ97>

© 2022 Jeff Kosseff.

<sup>†</sup> Associate Professor, Cyber Science Department, United States Naval Academy. The views in this Article are only the author’s and do not represent the Naval Academy, Department of Navy, or Department of Defense.

A.	ELIMINATING § 230 WON'T ELIMINATE THE FIRST AMENDMENT ..	789
B.	§ 230 PROVIDES CERTAINTY TO PLATFORMS.....	791
C.	§ 230 CARVEOUTS CAN HAVE SWEEPING IMPACTS.....	793
D.	“NEUTRALITY” IS ELUSIVE .....	795
E.	TRANSPARENCY COULD IMPROVE THE § 230 DEBATE.....	798
V.	CONCLUSION .....	801

## I. INTRODUCTION

In 2004, Orin Kerr undertook the vital but unenviable task of explaining the Stored Communications Act to the world. Earlier that year, the Ninth Circuit had issued an opinion that radically broke from previous judicial interpretations of the law, which governs service providers’ disclosure of customers’ emails and other communications records.<sup>1</sup> The Court had interpreted the statute in a way that expanded the types of communications to which it applied, using questionable analysis of key terms in the law. As Kerr observed, the misunderstandings of the Stored Communications Act were pervasive. “Despite its obvious importance, the statute remains poorly understood,” Kerr wrote. “Courts, legislators, and even legal scholars have had a very hard time making sense of the SCA.”<sup>2</sup>

Kerr’s article, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, has the primary goal of explaining “the basic structure and text of the Act so that legislators, courts, academics, and students can understand how it works—and in some cases, how it doesn’t work.” He also analyzes “how Congress should amend the statute in the future.”<sup>3</sup>

The article has achieved its purpose—in the eighteen years since its publication, dozens of judges have relied on Kerr’s article to help them interpret the Stored Communications Act’s murky provisions, including in some of the most important cases in the field.<sup>4</sup>

As I write this article in 2022, I feel the same sense of frustration that Kerr likely experienced, but not about the Stored Communications Act. In 2019, I published a book<sup>5</sup> about the history of § 230 of the Communications Decency

---

1. See *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004).

2. Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 (2004).

3. *Id.* at 1209.

4. See, e.g., *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008).

5. JEFF KOSSEFF, *THE TWENTY-SIX WORDS THAT CREATED THE INTERNET* (2019).

Act,<sup>6</sup> the statute that immunizes online platforms for liability arising from a great deal of user content. I argued that § 230 is responsible for the open Internet that Americans know today, as platforms are free to allow—or moderate—user content without fearing company-ending litigation.

Since I published the book, this once-obscure law has been thrust into the national spotlight, with calls to repeal the law from all sides of the political spectrum.<sup>7</sup> Some argue that large social media platforms have failed to remove harmful user-generated content. Others are upset that the platforms moderate too much speech and allegedly discriminate against particular political viewpoints.<sup>8</sup>

Section 230 has become a proxy for these complaints, even when § 230 is not directly related to the particular problem at hand. Politicians, commentators, scholars, and lobbyists are increasingly calling to amend or repeal § 230.<sup>9</sup> Although the § 230 debate has been loud, it has not been precise. Politicians and reporters have consistently misunderstood how the statute works and what it protects.<sup>10</sup>

---

6. 47 U.S.C. § 230.

7. See Lauren Feiner, *Biden Wants to Get Rid of Law that Shields Companies Like Facebook From Liability for What Their Users Post*, CNBC (Jan. 17, 2020) (“The bill became law in the mid-1990s to help still-nascent tech firms avoid being bogged down in legal battles. But as tech companies have amassed more power and billions of dollars, many lawmakers across the political spectrum along with Attorney General William Barr, agree that some reforms of the law and its enforcement are likely warranted.”).

8. See Danielle Keats Citron & Mary Anne Franks, *The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform*, 2020 U. CHI. LEGAL F. 45, 46–47 (2020) (“Today, politicians across the ideological spectrum are raising concerns about the leeway provided to content platforms under Section 230. Conservatives claim that Section 230 gives tech companies a license to silence speech based on viewpoint. Liberals criticize Section 230 for giving platforms the freedom to profit from harmful speech and conduct.”).

9. See, e.g., Dean Baker, *Getting Serious About Repealing Section 230*, CTR. FOR ECON. & POL’Y RSCH. (Dec. 18, 2020, 12:00 A.M.), <https://cepr.net/getting-serious-about-repealing-section-230/> (“I have argued that repeal would fundamentally change the structure of the industry, leading to a major downsizing of Facebook, Twitter, and other social media giants. It would also level the playing field between social media platforms and traditional media outlets.”).

10. See Ali Sternburg, *Why Do So Many Section 230 Stories Contain Corrections*, DISRUPTIVE COMPETITION PROJECT (Sept. 3, 2019), <https://www.project-disco.org/innovation/090319-why-do-so-many-section-230-stories-contain-corrections/> (“But for Section 230, online services could be sued by plaintiffs for removing anything from extremist content to pornography to fraudulent schemes. Section 230 also ensures that different services will take different approaches to content moderation. However, the frequency of inaccuracy in articles on this subject happens more often than one would expect for a law that is not that complex.”).

Consider the August 6, 2019, cover of the *New York Times* business section—published with the headline “Why Hate Speech on the Internet is a Never-Ending Problem.” Underneath that headline was the main twenty-six word provision of § 230 that provides immunity to online platforms for third-party content. Below that, the *Times* wrote, “Because this law shields it.” The *Times* soon published a correction for that statement: “An earlier version of this article incorrectly described the law that protects hate speech on the internet. The First Amendment, not Section 230, protects it.” Yet within weeks, a federal judge in New Jersey wrote about “Section 230’s grant of immunity for speech-based harms such as hate speech or libel” and cited the article.<sup>11</sup> Less than two years later, the *Times* ran another correction, this time for an article about former President Trump’s lawsuit against social media companies that suspended his account. The article “misidentified the legal provision that lets social media companies remove posts that violate their standards. It is the First Amendment, not Section 230.”<sup>12</sup>

This is a particularly unfortunate time for widespread misunderstandings about the statute. Congress is considering many proposals to amend or repeal § 230.<sup>13</sup> In 2018, Congress enacted the first-ever substantial amendment to the law, providing an exception for certain sex trafficking- and prostitution-related claims. Unfortunately, the widespread misunderstandings of § 230 may lead Congress to make changes that do not achieve their desired outcomes but instead threaten the freedoms that underpin the open internet that § 230 created in the United States.

Just as Kerr hoped to foster a more precise understanding of the Stored Communications Act, this Article aims to provide judges, the media, members of the public, and Congress with a better understanding of § 230’s purpose, mechanics, and impact. The Article debunks some of the most popular myths about § 230 and concludes by providing legislators with principles to guide the debate about the future of § 230 and content moderation.

Part II of the Article examines why Congress passed § 230 in 1996 and what the law actually says. To understand § 230’s purpose, it is necessary to review the First Amendment and common law protections for traditional

---

11. Order, *Papataros v. Amazon.com*, Civ. No. 17-9836 (D. N.J. Aug. 26, 2019).

12. Corrections, *N.Y. TIMES* (July 10, 2021).

13. See Cameron F. Kerry, *Section 230 Reform Deserves Careful and Focused Consideration*, BROOKINGS TECHTANK (May 14, 2021), <https://www.brookings.edu/blog/techtank/2021/05/14/section-230-reform-deserves-careful-and-focused-consideration/> (“[M]any blame Section 230 or seize on it as a vehicle to force changes on platforms. But there is little agreement among political leaders as to what are the real problems are, much less the right solutions. The result is that many proposals to amend or repeal Section 230 fail to appreciate collateral consequences—and would ultimately end up doing more harm than good.”).

distributors of speech, such as bookstores and newsstands. Section 230 helps fill in some gaps and uncertainties in those liability standards while also promoting growth and innovation of the nascent internet.

Part III explains how § 230 works in practice by outlining how courts have broadly interpreted the statute to immunize platforms in many contexts. It also describes how some plaintiffs have successfully circumvented § 230's liability protections.

Part IV charts a path forward, or at least provides principles to guide a path forward. Any changes to § 230 could have immediate and sweeping consequences, as seen after the 2018 sex trafficking amendment that caused many websites to change how they handle user content. Much of the debate has focused on repealing § 230 entirely. This Part explains why repealing § 230 would not necessarily solve many of the most significant problems that people have with social media. It instead outlines considerations to guide legislators as they determine whether and how to change § 230.

## II. WHY CONGRESS PASSED § 230

Congress passed § 230 in February 1996, at the dawn of the modern, commercial internet. The statute was intended to fill the gaps in the common law governing the liability of companies that distribute third-party content.<sup>14</sup> These rules were developed through decades of First Amendment cases concerning the liability of offline content distributors such as bookstores and newsstands. Although these legal rules worked relatively well in the pre-internet age, courts struggled to apply them to online services, as the following discussion illustrates.

### A. LIABILITY FOR DISTRIBUTORS BEFORE § 230

The most important case in the development of the common law distributor liability regime was *Smith v. California*, a 1959 U.S. Supreme Court opinion. The case involved Eleazar Smith, a Los Angeles bookstore owner who was convicted for selling a book in violation of an ordinance that prohibited booksellers from possessing indecent or obscene books.<sup>15</sup> Smith argued that the ordinance violated the First Amendment because it imposed “absolute” or “strict” liability on bookstore owners, no matter if they had any knowledge of the obscene material.

---

14. See KOSSEFF, *supra* note 5, at 57–78.

15. *Smith v. California*, 361 U.S. 147, 148 (1959).

The Supreme Court agreed with Smith. Eliminating any requirement for scienter “may tend to work a substantial restriction on the freedom of speech and of the press.”<sup>16</sup> Writing for the majority, Justice William Brennan acknowledged that the First Amendment does not protect obscenity, but he wrote that a strict liability ordinance would reduce the distribution of nonobscene, constitutionally protected books:

By dispensing with any requirement of knowledge of the contents of the book on the part of the seller, the ordinance tends to impose a severe limitation on the public’s access to constitutionally protected matter. For if the bookseller is criminally liable without knowledge of the contents, and the ordinance fulfills its purpose, he will tend to restrict the books he sells to those he has inspected; and thus the State will have imposed a restriction upon the distribution of constitutionally protected as well as obscene literature.<sup>17</sup>

Brennan recognized that opponents of the decision would argue that an obscenity statute with a scienter requirement would enable distributors to merely lie about whether they knew of or suspected illegality. But he believed that barrier could be overcome. “Eyewitness testimony of a bookseller’s perusal of a book hardly need be a necessary element in proving his awareness of its contents,” Brennan wrote. “The circumstances may warrant the inference that he was aware of what a book contained, despite his denial.”<sup>18</sup>

The Supreme Court explicitly avoided delving too deeply into the precise level of scienter that would satisfy the First Amendment, but it suggested possibilities such as: “whether honest mistake as to whether its contents in fact constituted obscenity need be an excuse; whether there might be circumstances under which the State constitutionally might require that a bookseller investigate further, or might put on him the burden of explaining why he did not, and what such circumstances might be.”<sup>19</sup> The Supreme Court’s holding in *Smith* would later be essential to its 1964 landmark ruling in *New York Times v. Sullivan*, in which it required public officials to demonstrate actual malice in libel lawsuits. “A rule compelling the critic of official conduct to guarantee the truth of all his factual assertions—and to do so on pain of libel judgments virtually unlimited in amount—leads to a comparable ‘self-censorship,’” the Court wrote.<sup>20</sup>

---

16. *Id.* at 151.

17. *Id.* at 153.

18. *Id.* at 154.

19. *Id.*

20. *N. Y. Times v. Sullivan*, 376 U.S. 254, 279 (1964).

The Court further refined its holding about distributor liability over the next decade. For instance, in a 1968 case, *Ginsberg v. New York*, the Supreme Court affirmed the constitutionality of a state law that penalized the sale of pornographic materials to minors, providing that the seller had “general knowledge of, or reason to know, or a belief or ground for belief which warrants further inspection or inquiry of both . . . the character and content of any material described herein which is reasonably susceptible of examination by the defendant” and the minor’s age.<sup>21</sup>

Relying on a New York state court opinion that had interpreted the same statute, the Supreme Court interpreted the statute to mean that “only those who are *in some manner aware* of the character of the material they attempt to distribute should be punished. It is not innocent but calculated purveyance of filth which is exorcised.”<sup>22</sup> Applying this definition, the Supreme Court held that it satisfied the *Smith v. California* scienter requirement. In other words, the Supreme Court does not necessarily require that an ordinance impose an actual knowledge requirement, but having a “reason to know” of the illegal content might suffice.

The First Amendment’s scienter requirement does not necessarily mean that the distributor must know or have reason to know that the content is illegal. In 1974, the Supreme Court in *Hamling v. United States* affirmed the convictions of criminal defendants for distributing obscene materials via the mail. The statute at issue applied to “[w]hoever knowingly uses the mails for the mailing . . . of anything declared by this section . . . to be nonmailable.”<sup>23</sup> The judge instructed the jury that to find the defendants guilty under this law, the jury must find that the defendants “knew the envelopes and packages containing the subject materials were mailed or placed . . . in Interstate Commerce, and . . . that they had knowledge of the character of the materials,” and that the defendants’ “belief as to the obscenity or non-obscenity of the material is irrelevant.”<sup>24</sup> The defendants argued that this instruction fell short of the First Amendment’s scienter requirements and that the prosecution required, “at the very least, proof both of knowledge of the contents of the material and awareness of the obscene character of the material.”<sup>25</sup>

The Supreme Court disagreed and held that the district court’s instructions met the minimum standards under the First Amendment. “It is constitutionally

---

21. *Ginsberg v. New York*, 390 US 629, 646 (1968) (emphasis in original).

22. *Id.* at 644.

23. *Hamling v. United States*, 418 U.S. 87, 119 (1974).

24. *Id.* at 119–20.

25. *Id.* at 120.

sufficient that the prosecution show that a defendant had knowledge of the contents of the materials he distributed, and that he knew the character and nature of the materials,” Justice Rehnquist wrote for the Court. “To require proof of a defendant’s knowledge of the legal status of the materials would permit the defendant to avoid prosecution by simply claiming that he had not brushed up on the law.”<sup>26</sup>

Scienter requirements for distributors extend beyond criminal obscenity cases. The Restatement (Second) of Torts incorporated a scienter requirement for defamation, stating 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.”<sup>27</sup> A comment to that rule states that a distributor “is not liable, if there are no facts or circumstances known to him which would suggest to him, as a reasonable man, that a particular book contains matter which upon inspection, he would recognize as defamatory.”<sup>28</sup>

The California Court of Appeal applied this rule in 1984 in a dispute involving Kenneth Osmond, the actor who played Eddie Haskell on *Leave it to Beaver*, and a chain of adult book stores. After the show went off the air, Osmond became a police officer in Los Angeles. Osmond learned that a chain of adult book stores, EWAP, was selling a pornographic film whose cover stated that the film’s male star was “John Holmes, who played ‘Little Eddie Haskell’ on the ‘Leave it to Beaver’ show.”<sup>29</sup> Osmond was the only actor to play Eddie Haskell; he had never been in pornography. Osmond sued the chain for libel. EWAP moved for summary judgment, arguing in part that the two store executives who ordered merchandise for the stores had not heard of Osmond, nor had they seen the carton that contained the allegedly defamatory claim.<sup>30</sup> The state trial court granted EWAP’s summary judgment motion, and the California Court of Appeal affirmed.

Relying on the Restatement and *Smith v. California*, the California Court of Appeal wrote that “in order to find the malice or scienter necessary to hold EWAP liable for disseminating the libelous material, a jury would be required to find that EWAP knew or had reason to know of its defamatory character.”<sup>31</sup> The court concluded that Osmond had not met that standard. “Since Osmond

---

26. *Id.* at 123.

27. Restatement (Second) of Torts § 581 (AM. L. INST. 1997).

28. *Id.* at cmt. e.

29. *Osmond v. EWAP*, 153 Cal. App. 3d 842, 847 (Cal. Ct. App. 1984).

30. *Id.* at 848.

31. *Id.* at 854.



did not present any evidence which makes us suspect that EWAP either had knowledge of the libel or was aware of information which imposed a duty to investigate, he did not make a sufficient showing of malice to justify consideration of the issue by the jury," the court wrote.<sup>32</sup>

Throughout the 1980s, only a handful of published opinions applied the distributor liability standard in defamation cases, and they articulated a similar rule: the liability of a distributor requires knowledge or reason to know of the defamatory or otherwise illegal content.<sup>33</sup> Distributor liability became a bit trickier to apply to the early 1990s commercial online services industry, which allowed customers to use dial-up modems to connect to bulletin boards and forums. These services, like bookstores, distributed content created by others. But the online services, even at that time, could have tens of thousands of users who each posted many messages a day. How did the distributor liability standards apply to these services?

The first case in which a judge attempted answer this question was *Cubby v. CompuServe* in 1991.<sup>34</sup> The plaintiffs sued CompuServe over allegedly defamatory statements that were published in a CompuServe forum a contractor managed for CompuServe.<sup>35</sup> A federal judge in the Southern District of New York granted CompuServe's summary judgment motion, applying the distributor liability framework and *Smith v. California* and its progeny.

First, the judge concluded that CompuServe was a distributor that was entitled to the same liability standards as a bookstore:

A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information.<sup>36</sup>

Had the judge not concluded that CompuServe was a distributor, it may have been just as liable for any defamation as the author of the article. The judge acknowledged that even a distributor such as CompuServe could have some control over the third-party content that it distributes because it can

---

32. *Id.* at 857.

33. *See, e.g.*, *Spence v. Flynt*, 647 F. Supp. 1266, 1273 (D. Wyo. 1986); *Dworkin v. Hustler*, 611 F. Supp. 781, 787 (D. Wyo. 1985).

34. *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991).

35. *Id.* at 137.

36. *Id.* at 140.

refuse to carry it: “While CompuServe may decline to carry a given publication altogether, in reality, once it does decide to carry a publication, it will have little or no editorial control over that publication’s contents.”<sup>37</sup> But because the judge concluded that CompuServe was a distributor, he ruled in the company’s favor, observing that the plaintiffs failed to produce “specific facts” that CompuServe “knew or had reason to know” about the contents of the forum.<sup>38</sup>

As Allen S. Hammond observed soon after the *Cubby* decision, editorial control appeared to be a key factor in determining an online service’s liability for third-party content. “The greater the discernable control that the system operator exercised over access and content, the greater its potential liability to users and third parties for damage caused by the information’s content,” Hammond wrote.<sup>39</sup>

The *Cubby* judge’s comment about “editorial control” ultimately would set the wheels in motion for § 230’s passage. Four years after the *CompuServe* dismissal, a New York state trial judge presided over a defamation lawsuit against CompuServe’s competitor, Prodigy. The case arose from user comments on a Prodigy financial discussion forum. The main distinction between CompuServe and Prodigy is that Prodigy had implemented user content guidelines, automatically screened user posts for offensive terms, and contracted with “Board Leaders” who enforced the user guidelines.<sup>40</sup>

The judge concluded that Prodigy was not a distributor like CompuServe but a publisher that faced the same liability as the comments’ author. Key to the judge’s decision were Prodigy’s attempts to moderate user content and that the company “held itself out as an online service that exercised editorial control over the content of messages posted on its computer bulletin boards, thereby expressly differentiating itself from its competition and expressly likening itself to a newspaper.”<sup>41</sup> Seizing on the distinction from *CompuServe*, the judge reasoned that whether Prodigy was a publisher or distributor hinged on whether the plaintiffs proved that it “exercised sufficient editorial control over its computer bulletin boards to render it a publisher with the same responsibilities as a newspaper.”<sup>42</sup>

---

37. *Id.*

38. *Id.* at 141.

39. Allen S. Hammond, *Private Networks, Public Speech: Constitutional Speech Dimensions of Access to Private Networks*, 55 U. PITT. L. REV. 1085, 1117–18 (1994).

40. *Stratton Oakmont v. Prodigy Servs Co.*, No. 31063/94, 1995 WL 323710, at \*1 (N. Y. Sup. Ct. May 24, 1995).

41. *Id.* at \*2.

42. *Id.* at \*3.

The judge found two main differences between CompuServe and Prodigy. “First, Prodigy held itself out to the public and its members as controlling the content of its computer bulletin boards,” the judge wrote. “Second, Prodigy implemented this control through its automatic software screening program, and the Guidelines which Board Leaders are required to enforce.”<sup>43</sup>

Because Prodigy wanted to “control” user content, the judge ruled, it must assume more liability for that content than a hands-off platform such as CompuServe.

“Presumably Prodigy’s decision to regulate the content of its bulletin boards was in part influenced by its desire to attract a market it perceived to exist consisting of users seeking a ‘family-oriented’ computer service,” the judge wrote. “This decision simply required that to the extent computer networks provide such services, they must also accept the concomitant legal consequences.”<sup>44</sup>

The opinion attracted immediate attention from the media and scholars. In an article published the day after the opinion’s release, the *New York Times* reported that an America Online lawyer “said she hoped that on-line services would not be forced to choose between monitoring bulletin boards and assuming liability for users’ messages.”<sup>45</sup> Norman Redlich and David R. Lurie wrote shortly after the opinion that the “divergent results” between the *Stratton Oakmont* and *CompuServe* cases “suggest a network operator will undertake substantial liability risks if it chooses to play any role in policing the content of communications on its system.”<sup>46</sup> Robert Hamilton, who successfully represented CompuServe in its defamation case, wrote that the *Stratton Oakmont* ruling was erroneously based on a dichotomy between “publishers” and “distributors” when, under the common law of libel, “the legal term ‘publisher’ includes both the person who creates the recorded defamatory text and the person who distributes it to others, but only when they have knowledge of the defamatory content that is disseminated.”<sup>47</sup> In other words, the editorial control that a platform exercises is not what determines whether a distributor is liable; instead, it is whether the distributor knows or has reason to know of the defamatory content.

---

43. *Id.* at \*4.

44. *Id.* at \*5.

45. Peter H. Lewis, *Judge Allows Libel Lawsuit Against Prodigy to Proceed*, N.Y. TIMES (May 26, 1995), <https://www.nytimes.com/1995/05/26/business/the-media-business-judge-allows-libel-lawsuit-against-prodigy-to-proceed.html>.

46. Norman Redlich & David R. Lurie, *First Amendment Issues Presented by the Information Superhighway*, 25 SETON HALL L. REV. 1446, 1458 (1994-1995).

47. Robert W. Hamilton, *Liability for Third-Party Content on the Internet*, 8 SETON HALL CONST. L. J. 733, 734 n.2 (1998).

In 1995, *Cubby* and *Stratton Oakmont* were the only U.S. court opinions that examined the liability of online services for the user content they distributed. Although these rulings were not binding on other courts, they were the only opinions that other judges could look to for guidance. And they suggested that platforms received greater liability protection if they took a hands-off approach to user content.

#### B. WHAT § 230 ACTUALLY SAYS

Congress was paying close attention in 1995 as it drafted the first overhaul of federal telecommunications laws in six decades. The new commercial internet was not the primary focus of the debate, with one significant exception. Members of Congress were concerned about the availability of pornography to minors who were accessing the internet from home, school, and libraries.<sup>48</sup> The July 3, 1995, cover of *Time* depicted a shocked child illuminated behind a keyboard, with the headline “Cyberporn.”<sup>49</sup>

To address this problem, Senator J. James Exon managed to add the Communications Decency Act (CDA) to the Senate’s version of the Telecommunications Act. The CDA would have imposed criminal penalties for the online transmission of indecent material to minors.<sup>50</sup> House members, however, had significant concerns about the constitutionality of the Act. House Speaker Newt Gingrich, at the time, stated that Exon’s bill was “clearly a violation of free speech and it’s a violation of the right of adults to communicate with each other.”<sup>51</sup>

Representatives Chris Cox and Ron Wyden took the lead in developing another way to help to reduce minors’ access to online pornography while also fostering the growth of the nascent commercial internet. They also sought to reverse the *Stratton Oakmont* decision,<sup>52</sup> which they saw as creating a perverse incentive for platforms to take an entirely hands-off approach to user content.

Representatives Cox and Wyden introduced the Internet Freedom and Family Empowerment Act<sup>53</sup> on June 30, 1995, a little over a month after the *Stratton Oakmont* decision. With some changes, the Act would eventually

---

48. See KOSSEFF, *supra* note 5, at 61-62.

49. TIME, July 3, 1995.

50. 141 Cong. Rec. S16006-07 (daily ed. 14, 1995) (statement of Sen. Exon).

51. Tim Murphy, *How Newt Gingrich Saved Porn*, MOTHER JONES (Dec. 2, 2011) <https://www.motherjones.com/politics/2011/12/how-newt-gingrich-saved-porn/>.

52. *Stratton Oakmont v. Prodigy Servs. Co.*, No. 31063/94, 1995 WL 323710, at \*1 (N.Y. Sup. Ct. May 24, 1995).

53. H.R. 1978, 104th Cong. (1995).

become what is now known as § 230.<sup>54</sup> The Act has two primary provisions, which at first were in the same paragraph, but throughout the legislative process were broken out into § 230 (c)(1) and § 230 (c)(2).

Section (c)(1) contains what I refer to as the twenty-six words that created the internet: “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.”<sup>55</sup> The Act broadly 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.”<sup>56</sup> Section 230 defines “information content provider” as “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.”<sup>57</sup>

As described in Part II, courts would soon interpret § 230(c)(1) to mean that platforms are not responsible for the content that their users post, whether or not they moderated user content. This would remove the specter of increased liability for platforms that exercise “editorial control,” as in *Stratton Oakmont*. Section 230(c)(1) only applies to information “that was “provided by another information content provider.” Thus, if the platform is “responsible, in whole or in part” for creating or developing content, § 230(c)(1) would not apply.

Section 230(c)(2) provides further protection for moderation, as well as for providing tools, such as website blockers, that allow users to control harmful content. The provision states that interactive computer service providers cannot be liable due to “any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected”<sup>58</sup> or enabling or providing “the technical means to restrict access” to such material.<sup>59</sup>

---

54. Unless otherwise noted, this Article quotes from the codified version of §230 rather than the introduced bill.

55. 47 U.S.C. § 230(c)(1).

56. 47 U.S.C. § 230(f)(2).

57. 47 U.S.C. § 230(f)(3).

58. 47 U.S.C. § 230(c)(2)(A).

59. 47 U.S.C. § 230(c)(2)(B).

Section 230 has exceptions for the enforcement of federal criminal law,<sup>60</sup> intellectual property law,<sup>61</sup> and electronic communications privacy laws.<sup>62</sup> The intellectual property law exception is particularly important to keep in mind, as some media coverage has incorrectly stated that § 230 protects platforms from copyright infringement claims.<sup>63</sup> (It is actually the Digital Millennium Copyright Act, an entirely different law, that sets the framework for platform liability arising from users' copyright infringement.)<sup>64</sup>

Section 230 does not exempt state criminal laws, though in 2018, Congress amended the law to create an exception for certain state criminal prosecutions involving sex trafficking and prostitution as well as some federal civil actions involving sex trafficking.<sup>65</sup>

Section 230 as introduced also prohibited the FCC from having authority over “economic or content regulation of the Internet or other interactive computer services.”<sup>66</sup> That provision would not remain in the final bill after conference committee, but it illustrated Representatives Cox and Wyden’s goal of fostering the internet by removing the threat of government regulation—a very different approach from Senator Exon’s bill.

To clarify their intentions, Representatives Cox and Wyden included statements of findings and policy in § 230. Among the findings of § 230 was that the “services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops”<sup>67</sup> and that they “offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.”<sup>68</sup> In line with the hands-off approach to the internet, § 230 includes a finding that online services “have flourished, to the benefit of all Americans, with a minimum of government regulation.”<sup>69</sup>

Section 230’s policy statement reflects similar goals for an unregulated internet that relies on the platforms to help users block objectionable content. Among the policies are “to promote the continued development of the

---

60. 47 U.S.C. § 230(e)(1).

61. 47 U.S.C. § 230(e)(2).

62. 47 U.S.C. § 230(e)(4).

63. See Mike Masnick, *NY Times Publishes A Second, Blatantly Incorrect, Trashing Of Section 230, A Day After Its First Incorrect Article*, TECHDIRT (Aug. 13, 2019).

64. 17 U.S.C. § 512.

65. 47 U.S.C. § 230(e)(5).

66. H.R. 1978, 104th Cong. § d (1995).

67. 47 U.S.C. § 230(a)(2).

68. 47 U.S.C. § 230(a)(3).

69. 47 U.S.C. § 230(a)(4).

Internet and other interactive computer services and other interactive media”;<sup>70</sup> “to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services”;<sup>71</sup> and “to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation.”<sup>72</sup>

Many of these findings and policy statements came from a 1995 report coordinated by the Center for Democracy and Technology, which urged “user empowerment” by providing parents with tools such as Net Nanny to block inappropriate online content.<sup>73</sup> The report highlighted the unconstitutionality of criminalizing indecent content, and it noted that the online services industry “is committed to developing more and better solutions, and the open nature of the Internet provides a wealth of possibilities for parental empowerment tools that may not yet have been imagined.”<sup>74</sup>

With this history in mind, it is important to point out that § 230 was intended to provide platforms with the flexibility to determine when and how to moderate user content. As discussed in Part III, some participants in the current debate about § 230 have incorrectly suggested that it only applies to “neutral platforms.” To the contrary, Congress wanted to pass a law to overturn *Stratton Oakmont* and ensure that platforms did *not* have an incentive to be neutral.

This goal was clear when the bill came up for House floor debate on August 4, 1995, as an amendment to the House’s version of the telecommunications overhaul. Representative Cox emphasized the “backward” nature of the *Stratton Oakmont* ruling and argued the bill would:

[P]rotect computer Good Samaritans, online service providers, anyone who provides a front end to the Internet, let us say, who takes steps to screen indecency and offensive material for their customers. It will protect them from taking on liability such as occurred in the Prodigy case in New York that they should not face for helping us and for helping us solve this problem.<sup>75</sup>

---

70. 47 U.S.C. § 230(b)(1).

71. 47 U.S.C. § 230(b)(3).

72. 47 U.S.C. § 230(b)(2).

73. INTERACTIVE WORKING GROUP REPORT, PARENTAL EMPOWERMENT, CHILD PROTECTION, AND FREE SPEECH IN INTERACTIVE MEDIA (1995).

74. *Id.*

75. 104 Cong. Rec. H8470 (daily ed. Aug. 4, 1995) (statement of Rep. Cox).

But Representative Cox also articulated a second goal:

[To] establish as the policy of the United States that we do not wish to have content regulation by the Federal Government of what is on the Internet, that we do not wish to have a Federal Computer Commission with an army of bureaucrats regulating the Internet because frankly the Internet has grown up to be what it is without that kind of help from the Government.<sup>76</sup>

Representative Robert Goodlatte emphasized the impracticality of holding service providers liable for all of their user content:

There is no way that any of those entities, like Prodigy, can take the responsibility to edit out information that is going to be coming into them from all manner of sources onto their bulletin board. We are talking about something that is far larger than our daily newspaper. We are talking about something that is going to be thousands of pages of information every day, and to have that imposition imposed on them is wrong.<sup>77</sup>

The Cox-Wyden amendment was positioned as the alternative to Senator Exon's Communications Decency Act. Representative Zoe Lofgren spoke in favor of the Cox-Wyden amendment, arguing that Exon's bill "is like saying that the mailman is going to be liable when he delivers a plain brown envelope for what is inside it."<sup>78</sup>

The House voted 420-4 to add § 230 to its telecommunications reform bill.<sup>79</sup> Both the Senate's Communications Decency Act and Cox and Wyden's § 230 were included in the final, negotiated telecommunications bill signed into law in February 1996.

Perhaps § 230's prohibition on FCC regulation of internet content was removed from the final bill because it might have conflicted with the Communications Decency Act, but there is no record as to the reasoning for that change. The conference committee did, however, write in the conference report that it intended to overrule *Stratton Oakmont* "and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material."<sup>80</sup> To clarify Section 230's impact on litigation, the enacted law contains a provision that was not in the introduced bill, stating

---

76. *Id.*

77. *Id.* at H8471.

78. *Id.*

79. *Id.* at H8478.

80. H. R. Rep. No. 104-458, at 194 (1996).



that “[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.”<sup>81</sup>

Because § 230 was placed in the same part of the telecommunications law as the Communications Decency Act, it became known as § 230 of the Communications Decency Act, even though it would be more accurate to call the provision § 230 of the Communications Act of 1934.<sup>82</sup> A year later, the Supreme Court struck down as unconstitutional the Senate’s Communications Decency Act, which penalized the transmission of indecent materials.<sup>83</sup> But the opinion did not affect § 230, as it did not involve imposing penalties for the distribution of constitutionally protected speech.

### III. HOW § 230 WORKS

When Congress passed § 230, the liability protections of § 230(c)(1) and § 230(c)(2) received little public attention. Most of the media attention focused on Exon’s Communications Decency Act, and the Telecommunications Act of 1996 was portrayed as a loss for civil liberties advocates and technology companies.<sup>84</sup> The lack of attention to § 230 likely was at least partly because it was unclear how courts would interpret the statute. It would take another year for courts to determine that § 230(c)(1) provides platforms with extraordinarily broad protections.

#### A. THE BROAD SCOPE OF § 230(c)(1)

There are at least two ways to read the twenty-six words of § 230(c)(1). A limited reading would conclude that prohibiting interactive computer service providers from being “treated” as publishers or speakers of third-party content means that all such providers are instead treated as distributors.<sup>85</sup> Under that

---

81. 47 U.S.C. § 230(e).

82. For an exhaustive discussion of § 230’s name, see Blake Reid, *Section 230 of . . . What?* (Sept. 4, 2020), <https://blakereid.org/section-230-of-what/>.

83. *Reno v. American Civil Liberties Union*, 521 U.S. 844, 885 (1997) (“The record demonstrates that the growth of the Internet has been and continues to be phenomenal. As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it.”).

84. See Howard Bryant & David Plotnikoff, *How the Decency Fight Was Won*, SAN JOSE MERCURY NEWS (Mar. 3, 1996) (stating that the “Internet’s free speech supporters lost their historic battle over cyberspace decency standards because they were outgunned, outflanked, out-connected and out-thought in the most crucial battle of the online community’s brief history”).

85. See Ian Ballon, *Zeran v. AOL: Why the Fourth Circuit Is Wrong*, J. INTERNET L. (1998) (“In this author’s view, Congress effectively codified an altered version of the *Cubby* standard

reading, a platform would be liable for user content if it knew or had reason to know of the defamatory or otherwise illegal content. In other words, if a platform received a complaint alleging that user content was defamatory, the platform would either need to take down the content or defend a defamation suit just as the author would. A platform also might be liable even without having received a complaint, though the lack of on-point caselaw makes it difficult to predict how a court would determine when a platform had a “reason to know” of the content.

A second, broader, reading would interpret § 230(c)(1) as barring any claim against an interactive computer service provider arising from third-party content unless an exception applied. This would mean that even if a platform knew or had reason to know of defamatory user content, it would not be liable for that content. Such a reading would require a court to conclude that treating a platform as a distributor would fall under § 230’s prohibition of treatment as a publisher. In other words, the broader interpretation of § 230 requires courts to consider a distributor as a type of publisher.

The first federal appellate court to interpret § 230(c)(1) adopted the broader reading. On November 12, 1997, the Fourth Circuit issued its opinion in *Zeran v. America Online*. The case involved offensive posts on an AOL bulletin board that purported to sell t-shirts with tasteless jokes about the recent Oklahoma City bombing. The posts instructed readers to call “Ken” at a Seattle phone number that belonged to Ken Zeran.<sup>86</sup> Zeran, who had nothing to do with the advertisements and did not even have an AOL account, received many angry calls and death threats.<sup>87</sup> Zeran repeatedly contacted AOL about the ads, but the company failed to promptly remove them or prevent their reposting.<sup>88</sup>

Zeran sued AOL for negligence. The common law and First Amendment defense for distributors likely would not have succeeded for AOL, as Zeran’s claims arose from AOL’s failure to remove and prevent the postings *after* he informed the company of them. Thus, AOL defended itself on the basis that § 230 immunized it from Zeran’s lawsuit. But the only way that this defense would work is if the court agreed with the broader interpretation of § 230: that

---

under which a service provider (or user) may be held indirectly liable for third party acts of defamation only in instances where it actually knew that material posed online was defamatory and failed to take any action, or in very limited circumstances where it failed to act despite reason to know that material was defamatory (provided that the basis for imputed knowledge is not the provider’s acts of monitoring online content).”).

86. *Zeran v. America Online*, 129 F.3d 327, 329 (4th Cir. 1997).

87. *Id.*

88. *Id.*

it not only prevented interactive computer service provider from being treated as publishers but also as distributors.

The district court agreed with AOL's broad reading of § 230 and dismissed the case, writing that "distributor liability, or more precisely, liability for knowingly or negligently distributing defamatory material, is merely a species or type of liability for publishing defamatory material."<sup>89</sup> Zeran appealed, and the Fourth Circuit affirmed the dismissal and the broad reading of §230's liability protections.

Writing for the unanimous three-judge panel, Judge J. Harvie Wilkinson observed that Congress passed § 230 to foster open and free discourse on the internet:

Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum.<sup>90</sup>

Wilkinson agreed with the district court that § 230 precludes notice-based liability for distributors. "The simple fact of notice surely cannot transform one from an original publisher to a distributor in the eyes of the law," Wilkinson wrote. "To the contrary, once a computer service provider receives notice of a potentially defamatory posting, it is thrust into the role of a traditional publisher."<sup>91</sup>

Wilkinson also recognized the burdens on free speech that distributor liability would create and wrote that such a chilling effect would conflict with § 230's purpose: "If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement—from any party, concerning any message." According to Wilkinson, "Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information."<sup>92</sup>

---

89. Zeran v. America Online, 958 F. Supp. 1124, 1133 (E.D. Va. 1997).

90. Zeran v. America Online, 129 F.3d 327, 330 (4th Cir. 1997).

91. *Id.* at 332.

92. *Id.* at 333.

Allowing platforms to become liable upon notice, Wilkinson wrote, would allow plaintiffs to effectively veto online speech that they want removed from the internet.<sup>93</sup> Congress, he wrote, did not intend such an outcome. “Whenever one was displeased with the speech of another party conducted over an interactive computer service, the offended party could simply ‘notify’ the relevant service provider, claiming the information to be legally defamatory,” Wilkinson wrote. “In light of the vast amount of speech communicated through interactive computer services, these notices could produce an impossible burden for service providers, who would be faced with ceaseless choices of suppressing controversial speech or sustaining prohibitive liability.” Wilkinson read § 230(c)(1) as immunizing platforms for a wide range of activities that publishers perform, including “deciding whether to publish, withdraw, postpone or alter content.”<sup>94</sup>

Wilkinson’s ruling soon attracted some criticism from scholars who argued that Congress only intended to impose distributor liability; it did not intend an absolute bar to liability even if the platforms knew or had reason to know of the defamatory or illegal content.<sup>95</sup>

With no other guidance from federal appellate courts, judges nationwide soon adopted Wilkinson’s broad reading of § 230. For instance, in 1998, Judge Paul Friedman of the U.S. District Court for the District of Columbia dismissed a lawsuit against AOL for an allegedly defamatory Matt Drudge column that AOL distributed. The plaintiff argued that § 230 did not apply. Quoting extensively from Wilkinson’s opinion, Friedman wrote that the “court

---

93. *Id.* at 330.

94. *Id.*

95. See, e.g., David R. Sheridan, *Zeran v. AOL and the Effect of Section 230 of the Communications Decency Act Upon Liability for Defamation on the Internet*, 61 ALB. L. REV. 147, 151 (1997) (writing of the district court’s dismissal in the *Zeran* case: “It can be argued that the *Zeran* holding is supported neither by the text of the law nor by the legislative history expressing an intent to overrule *Stratton Oakmont*. However, the *Zeran* holding is arguably consistent with Congress’s intent, expressed in the CDA itself, to put control over content in the hands of users of interactive computer services and of parents of minor users.”); Todd G. Hartman, *Marketplace vs. the Ideas: The First Amendment Challenges to Internet Commerce*, 12 HARV. J. L. & TECH. 419, 446-47 (1999) (“Thus, despite clear legal precedent arguing for a narrow interpretation of section 230, the court extended the scope of section 230 to provide AOL immunity from distributor liability as well as publisher liability. In doing so, the *Zeran* court ignored the specific intent of Congress in passing section 230, which was to facilitate the restriction of offensive material, not restrict its dissemination.”). *Contra* Cecilia Ziniti, *Optimal Liability System for Online Service Providers: How Zeran v. America Online Got It Right and Web 2.0 Proves It*, 23 BERKELEY TECH. L.J. 583 (2008) (highlighting the chilling effects of a distributor liability system and arguing that “*Zeran* has proven efficient and adaptable and nurtured the growth of beneficial innovation online”).

in *Zeran* has provided a complete answer to plaintiffs' primary argument, an answer grounded in the statutory language and intent of Section 230."<sup>96</sup> Likewise, in 2000, the Tenth Circuit affirmed the dismissal of a lawsuit against AOL for distributing allegedly inaccurate stock information, citing *Zeran* for the proposition that "Congress clearly enacted § 230 to forbid the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions."<sup>97</sup> As Eric Goldman wrote in 2017, *Zeran* is "the most important Section 230 ruling to date-and probably the most important court ruling in Internet Law."<sup>98</sup>

Although the floor debate about § 230 did not directly address whether Congress intended the broad reading that Wilkinson applied, it is noteworthy that in a report accompanying a 2002 children's online safety law, the House Committee on Energy and Commerce, citing *Zeran* and other early opinions that relied on its reasoning, wrote that "[t]he courts have correctly interpreted section 230(c), which was aimed at protecting against liability for such claims as negligence."<sup>99</sup> Likewise, both Representatives Cox and Wyden have said that the *Zeran* interpretation was correct.<sup>100</sup>

Under the *Zeran* rule, as interpreted by other courts, even platforms that encourage users to post scurrilous content receive § 230 protections. For instance, in *Jones v. Dirty World Entertainment Recordings*, a website called TheDirty.com invited users to provide "dirt" on others via a submission form that said, "Tell us what's happening. Remember to tell us who, what, when, where, why."<sup>101</sup> The website's staff selected about 150 to 200 of the thousands of daily submissions for posting, and they all were signed "THE DIRTY ARMY."<sup>102</sup> The site's operator, Nik Richie, often added a short humorous comment beneath the user submission.<sup>103</sup> TheDirty users posted a number of submissions about Sarah Jones, a high school teacher and NFL cheerleader, including allegations that she slept with football players and had a sexually

---

96. *Blumenthal v. Drudge*, 992 F. Supp. 44, 51 (D.D.C. 1998).

97. *Ben Ezra, Weinstein, & Co. v. America Online*, 206 F.3d 980, 986 (10th Cir. 2000).

98. Eric Goldman, *The Ten Most Important Section 230 Rulings*, 20 TUL. J. TECH. & INTELL. PROP. 1, 3 (2017).

99. H.R. Rep. No. 107-449, at 13 (2002).

100. See KOSSEFF, *supra* note 5, at 95; Brief for Chris Cox, Former Member of Congress and Co-Author of CDA Section 230, and Netchoice as *Amici Curiae* Supporting Defendants and Affirmance at 23, *La Park La Break LLC v. Airbnb, Inc.*, No. 18-55113 (9th Cir. Sept. 27, 2018).

101. *Jones v. Dirty World Ent. Recordings*, 755 F.3d 398, 402-03 (6th Cir. 2014).

102. *Id.* at 403.

103. *Id.*

transmitted disease.<sup>104</sup> Beneath one of the posts, Richie wrote, “Why are all high school teachers freaks in the sack?”<sup>105</sup> Despite Jones’ repeated pleas, the website refused to remove the posts.<sup>106</sup> She sued the website for defamation, false light, and intentional infliction of emotional distress.<sup>107</sup>

The district court refused to dismiss the case under § 230, reasoning that “a website owner who intentionally encourages illegal or actionable third-party postings to which he coadds his own comments ratifying or adopting the posts becomes a ‘creator’ or ‘developer’ of that content and is not entitled to immunity.”<sup>108</sup> The case went to trial and led to a \$338,000 verdict for Jones.<sup>109</sup> But the Sixth Circuit reversed the verdict, holding that § 230 did in fact immunize the website. In line with other circuits, the Sixth Circuit ruled that a website has developed content for the purposes of § 230 if it has made a “material contribution to the alleged illegality of the content,” meaning that it is “responsible for what makes the displayed content allegedly unlawful.”<sup>110</sup> Merely encouraging the content, the Sixth Circuit held, was not enough to constitute “development” under § 230:

Many websites not only allow but also actively invite and encourage users to post particular types of content. Some of this content will be unwelcome to others — e.g., unfavorable reviews of consumer products and services, allegations of price gouging, complaints of fraud on consumers, reports of bed bugs, collections of cease-and-desist notices relating to online speech. And much of this content is commented upon by the website operators who make the forum available. Indeed, much of it is “adopted” by website operators, gathered into reports, and republished online. Under an encouragement test of development, these websites would lose the immunity under the CDA and be subject to hecklers’ suits aimed at the publisher.<sup>111</sup>

---

104. *Id.*

105. *Id.* at 404.

106. *Id.*

107. *Id.* at 405.

108. *Id.* at 409.

109. *Id.* at 405–06.

110. *Id.* at 410.

111. *Id.* at 414.

*Jones* received substantial media and scholarly attention, with some arguing that § 230 should not protect sites such as TheDirty<sup>112</sup> and others asserting that the Sixth Circuit correctly interpreted the statute.<sup>113</sup>

The vast majority of § 230-related dismissals involve § 230(c)(1), including decisions not only to keep material up but to take material down. In a 2020 review of more than 500 § 230 decisions over two decades, the Internet Association found only nineteen involved § 230(c)(2).<sup>114</sup> As the Ninth Circuit wrote in 2009, § 230(c)(1) “shields from liability all publication decisions, whether to edit, to remove, or to post, with respect to content generated entirely by third parties.”<sup>115</sup> Section 230(c)(2)’s protections for good-faith actions to remove objectionable content, the court wrote, could apply to interactive computer service providers who are not necessarily covered by § 230(c)(1). “Thus, even those who cannot take advantage of subsection (c)(1), perhaps because they developed, even in part, the content at issue, can take advantage of subsection (c)(2) if they act to restrict access to the content because they consider it obscene or otherwise objectionable,” the Court wrote.<sup>116</sup> “Additionally, subsection (c)(2) also protects internet service providers from liability not for publishing or speaking, but rather for actions taken to restrict access to obscene or otherwise objectionable content.”<sup>117</sup>

#### B. WORKING AROUND § 230(c)(1)

Courts have imposed some limits on the application of § 230(c)(1)’s broad immunity. Judges have denied § 230(c)(1) protection in two situations: (1) where the platform at least partly developed or created the content; and (2)

---

112. See Laura Cannon, *Indecent Communications: Revenge Porn and Congressional Intent of Sec. 230(c)*, 90 TUL. L. REV. 471, 490 (2015) (“The Sixth Circuit, commentators, scholars, and interested parties failed to distinguish between websites that solicit user input to gauge services or promote consumer confidence and websites that exist solely to elicit tortious content.”).

113. See Christine N. Walz & Robert L. Rogers II., *Sixth Circuit’s Decision in Jones v. Dirty World Entertainment Recordings LLC Repairs Damage to Communications Decency Act*, 30 COMM. LAW. 4 (2014) (“The Sixth Circuit has therefore not overreached, and has retained adequate remedies for the victims of defamation that more accurately fulfill the congressional intent behind § 230 of the CDA.”).

114. ELIZABETH BANKER, INTERNET ASSOCIATION, A REVIEW OF SECTION 230’S MEANING & APPLICATION BASED ON MORE THAN 500 CASES (July 27, 2020) (“Of these, the vast majority involved disputes over provider efforts to block spam. The remainder were resolved under Section 230(c)(1), Anti-SLAPP motions, the First Amendment, or for failure to state a claim based on other deficiencies.”).

115. *Barnes v. Yahoo! Inc.*, 570 F.3d 1096, 1105 (9th Cir. 2009).

116. *Id.* (internal citations omitted).

117. *Id.* (internal citations omitted).

where the claim did not treat the platform as the publisher or speaker of third-party content.

1. *Development or Creation of Content*

Section 230(c)(1) only applies to information provided by *another* information content provider, which the statute defines as a person or entity “that is responsible, in whole or in part, for the creation or development of information.”<sup>118</sup> Thus, if the platform itself is even partly responsible for creating or developing content, it cannot claim § 230 protections for that content.

In perhaps the most influential opinion to narrow some of § 230’s protections, the Ninth Circuit, sitting en banc in 2008, partly refused to immunize a roommate-matching website, Roommates.com, for alleged violations of federal and state housing laws. The alleged violations arose from Roommates.com’s user-registration process, which required users to complete a questionnaire for users to provide demographic information, such as sexual orientation and sex, and indicate their preferences from a list of demographic categories.<sup>119</sup>

The Ninth Circuit ruled that § 230 did not apply to claims arising from any allegedly discriminatory questions that the websites asked. “The CDA does not grant immunity for inducing third parties to express illegal preferences. Roommate’s own acts—posting the questionnaire and requiring answers to it—are entirely its doing and thus § 230 of the CDA does not apply to them,” the Court wrote.<sup>120</sup> The majority reasoned that if a real estate broker is prohibited from asking about a prospective buyer’s race, an online platform faces that same prohibition.<sup>121</sup>

Likewise, the Ninth Circuit concluded that § 230 did not immunize the website from claims arising from the “development and display of subscribers’ discriminatory preferences.”<sup>122</sup> The court reasoned that this allegedly discriminatory content comes directly from the mandatory registration process. “By requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated

---

118. 47 U.S.C. 230(f)(3).

119. *Fair Hous. Council of San Fernando Valley v. Roommates.com*, 521 F.3d 1157, 1161-62 (9th Cir. 2008) (en banc).

120. *Id.* at 1165.

121. *Id.* at 1164 (“If such questions are unlawful when posed face-to-face or by telephone, they don’t magically become lawful when asked electronically online. The Communications Decency Act was not meant to create a lawless no-man’s-land on the Internet.”).

122. *Id.*



answers, Roommate [sic] becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information,” the Court wrote.<sup>123</sup>

But the Ninth Circuit did not entirely deny § 230 protection to Roommates.com. The Court held that § 230 applied to any allegedly discriminatory statements in the freeform “Additional Comments” section of user profiles. “The fact that Roommate [sic] encourages subscribers to provide something in response to the prompt is not enough to make it a ‘develop[er]’ of the information under the common-sense interpretation of the term we adopt today,” the Court wrote.<sup>124</sup>

“It is entirely consistent with Roommate’s [sic] business model to have subscribers disclose as much about themselves and their preferences as they are willing to provide,” the Court added.<sup>125</sup> “But Roommate [sic] does not tell subscribers what kind of information they should or must include as ‘Additional Comments,’ and certainly does not encourage or enhance any discriminatory content created by users.”<sup>126</sup>

As the majority summarized in *Roommates.com*, “a website helps to develop unlawful content, and thus falls within the exception to § 230, if it contributes materially to the alleged illegality of the content.”<sup>127</sup> Dissenting, Judge McKeown wrote that the majority misinterpreted § 230. “The plain language and structure of the CDA unambiguously demonstrate that Congress intended these activities—the collection, organizing, analyzing, searching, and transmitting of third-party content—to be beyond the scope of traditional publisher liability,” the judge wrote. “The majority’s decision, which sets us apart from five circuits, contravenes congressional intent and violates the spirit and serendipity of the Internet.”<sup>128</sup>

Still, other courts adopted the majority’s narrower reading of § 230. The next year, the Tenth Circuit adopted the material contribution test and concluded that § 230 did not protect the operator of a website from a Federal Trade Commission lawsuit alleging that third-party researchers used the

---

123. *Id.* at 1166.

124. *Id.* at 1172.

125. *Id.* at 1174.

126. *Id.*

127. *Id.* at 1168.

128. *Id.* at 1177 (McKeown, J., concurring in part and dissenting in part).

website to provide consumers with material that allegedly violated privacy laws.<sup>129</sup>

*Roommates.com* is one of the most cited § 230 opinions and was the first clear recognition that courts would restrict § 230.<sup>130</sup> But in more than a decade since the opinion, other courts have used its reasoning relatively sparingly to deny § 230 protections. As Eric Goldman observed, “most courts have read *Roommates.com*’s exception to Section 230 fairly narrowly.”<sup>131</sup>

## 2. *Treatment as Publisher or Speaker*

Some courts have also concluded that § 230 does not apply because the lawsuits do not seek to treat the interactive computer service providers as publishers or speakers of third-party content.

This § 230 workaround was first prominently displayed in a 2009 Ninth Circuit case, *Barnes v. Yahoo*. The plaintiff’s ex-boyfriend allegedly posted explicit images of her on a Yahoo dating website, also listing her contact information.<sup>132</sup> This caused men to visit and contact her at work, seeking sex.<sup>133</sup> The plaintiff complied with Yahoo’s intricate complaint process to have the profile removed, but the company did not respond.<sup>134</sup> After a local television show began to prepare a story about the plaintiff’s situation, a Yahoo executive told the plaintiff to fax them the necessary information and they would “personally walk the statements over to the division responsible for stopping unauthorized profiles and they would take care of it.”<sup>135</sup> The plaintiff faxed the

---

129. See *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1200 (10th Cir. 2009) (“By paying its researchers to acquire telephone records, knowing that the confidentiality of the records was protected by law, it contributed mightily to the unlawful conduct of its researchers. Indeed, Accusearch’s responsibility is more pronounced than that of *Roommates.com*. *Roommates.com* may have encouraged users to post offending content; but the offensive postings were Accusearch’s *raison d’etre* and it affirmatively solicited them.”).

130. See Mary Graw Leary, *The Indecency and Injustice of Section 230 of the Communications Decency Act*, 41 HARV. J. L. & PUB. POL’Y 553, 576 (2018) (“[H]olding that *Roommates.com* was a content provider made it one of the few cases to find potential liability for a website. In so doing it recognized a website could be both an interactive computer service as well as a content provider, at least where the website helped to develop the information . . .”).

131. Eric Goldman, *The Ten Most Important Section 230 Rulings*, 20 TUL. J. TECH. & INTELL. PROP. 1, 4 (2017) (“The opinion emphatically says the following: ‘If you don’t encourage illegal content, or design your website to require users to input illegal content, you will be immune.’ Perhaps surprisingly, many courts have cited this *Roommates.com* language while ruling in favor of Section 230 immunity.”).

132. *Barnes v. Yahoo! Inc.*, 570 F.3d 1096, 1098 (9th Cir. 2009).

133. *Id.*

134. *Id.*

135. *Id.* at 1099.

necessary information, but she did not hear back from Yahoo. Two months later, she sued Yahoo for negligent undertaking and promissory estoppel.<sup>136</sup> The district court dismissed the entire lawsuit under § 230.<sup>137</sup>

On appeal, the Ninth Circuit affirmed the § 230-based dismissal of the negligent undertaking claim.<sup>138</sup> But the Ninth Circuit reversed the dismissal of the promissory estoppel claim, reasoning that the plaintiff “d[id] not seek to hold Yahoo liable as a publisher or speaker of third-party content, but rather as the counter-party to a contract, as a promisor who has breached.”<sup>139</sup> Making a promise, the Court wrote, “is different because it is not synonymous with the performance of the action promised. That is, whereas one cannot undertake to do something without simultaneously doing it, one can, and often does, promise to do something without actually doing it at the same time.”<sup>140</sup>

In other words, § 230 did not protect Yahoo from a promissory estoppel claim because the success of the claim did not require Yahoo to be treated as the publisher or speaker of third-party content. This is different from the *Roommates.com* reasoning, which avoids § 230 protections due to the platform’s material contribution to the creation of the illegality.

More recently, in 2016, the Ninth Circuit reversed the § 230 dismissal of a lawsuit against Internet Brands, the operator of a modeling website. The site enabled models to post profiles for talent scouts.<sup>141</sup> The plaintiff was contacted by a man, purporting to be a talent scout, who later drugged and raped her with another man.<sup>142</sup> The plaintiff, Jane Doe, alleged that Internet Brands had known about the two men previously using the site to identify women who they would later rape.<sup>143</sup>

The Ninth Circuit reversed the district court’s § 230 dismissal of the case, reasoning that Jane Doe’s lawsuit did not treat Internet Brands as the publisher or speaker of third-party content. The plaintiff was not seeking to hold

---

136. *Id.*

137. *Id.*

138. *Id.* at 1103 (“In other words, the duty that Barnes claims Yahoo violated derives from Yahoo’s conduct as a publisher—the steps it allegedly took, but later supposedly abandoned, to de-publish the offensive profiles. It is because such conduct is publishing conduct that we have insisted that section 230 protects from liability any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online.”) (internal quotation marks and citation omitted).

139. *Id.* at 1107.

140. *Id.*

141. *Doe v. Internet Brands*, 824 F.3d 846, 848 (9th Cir. 2016).

142. *Id.* at 849.

143. *Id.*

Internet Brands liable for the profile that she posted, nor did her lawsuit allege that the men had posted content on the site, the Court noted.<sup>144</sup>

“Instead, Jane Doe attempts to hold Internet Brands liable for failing to warn her about information it obtained from an outside source about how third parties targeted and lured victims through Model Mayhem,” the Court wrote. “The duty to warn allegedly imposed by California law would not require Internet Brands to remove any user content or otherwise affect how it publishes or monitors such content.”<sup>145</sup>

The Ninth Circuit extended this somewhat more limited reading of § 230 in *Lemmon v. Snap*.<sup>146</sup> The plaintiffs were parents of two teenagers who died in a car accident. They alleged that their sons were using a Snapchat function known as “Speed Filter,” which allows users to take photos or videos while recording the speed at which they are traveling.<sup>147</sup> Many Snapchat users allegedly played a game in which they tried to record a speed at 100 miles per hour or greater. The plaintiffs’ sons were traveling at up to 123 miles per hour before their car crashed.<sup>148</sup>

The parents sued Snap for negligent design, but the district court dismissed the case based on § 230. The Ninth Circuit reversed the dismissal, reasoning that the lawsuit did not treat Snap as the publisher or speaker of third-party content. “To the extent Snap maintains that CDA immunity is appropriate because the Parents’ claim depends on the ability of Snapchat’s users to use Snapchat to communicate their speed to others, it disregards our decision in *Internet Brands*,” the Ninth Circuit wrote. “That Snap allows its users to transmit user-generated content to one another does not detract from the fact that the Parents seek to hold Snap liable for its role in violating its distinct duty to design a reasonably safe product.”

The “no treatment as a publisher” claims have not always succeeded. For instance, in 2017, Matthew Herrick sued Grindr after his ex-boyfriend used the dating app to impersonate Herrick and post profiles stating that he was interested in “serious kink and many fantasy scenes,” causing more than 1,000 people to respond, with many arriving at his home and work due to Grindr’s geolocation function.<sup>149</sup> Despite receiving more than 100 complaints from Herrick and others about these fake accounts, Grindr did nothing other than

---

144. *Id.* at 851.

145. *Id.*

146. *Lemmon v. Snap*, 995 F.3d 1085 (9th Cir. 2021).

147. *Id.*

148. *Id.*

149. *Herrick v. Grindr, LLC*, 306 F. Supp. 3d 579, 585 (S.D.N.Y. 2018).

send an automated reply, Herrick's complaint alleged.<sup>150</sup> Herrick's lawsuit against Grindr focused on the dangerous nature of the app and the failure to incorporate basic safety features. The lawsuit included claims for negligence, deceptive business practices and false advertising, emotional distress, failure to warn, negligent misrepresentation, products liability, negligent design, promissory estoppel, and fraud.<sup>151</sup>

Relying on the Ninth Circuit's *Internet Brands* opinion, Herrick argued that § 230 did not apply to his failure to warn claim, but the district court rejected the comparison. "By contrast, the proposed warning in this case would be about user-generated content itself—the impersonating profiles or the risk that Grindr could be used to post impersonating or false profiles," the district court wrote.<sup>152</sup> "Unlike in *Internet Brands*, Herrick's failure-to-warn claim depends on a close connection between the proposed warning and user-generated content."<sup>153</sup> The district court concluded that the other claims were either also immunized under § 230 or inadequately pled.<sup>154</sup> The Second Circuit affirmed the district court's dismissal in a nonprecedential summary order,<sup>155</sup> and the U.S. Supreme Court denied certiorari.<sup>156</sup>

### C. JUDICIAL CALLS FOR § 230 REFORM

Despite the abrogation of § 230 at the edges, Judge Wilkinson's primary holding in *Zeran*—that the prohibition on treating interactive computer service providers as publishers includes a ban on distributor liability—has gone largely unchallenged by judges over the past quarter century. The Supreme Court has never interpreted the scope of § 230, but Justice Thomas appears eager not only to take a § 230 case, but to challenge the broad *Zeran* reading of the statute. In a 2020 statement accompanying the Supreme Court's denial of certiorari in a case involving § 230(c)(2), Justice Thomas wrote that "there are good reasons to question" the broad *Zeran* reading that extends § 230(c)(1) to distributor liability.<sup>157</sup> He also criticized courts' broad application of § 230. "Paring back the sweeping immunity courts have read into § 230 would not necessarily render defendants liable for online misconduct," Thomas wrote.

---

150. *Id.*

151. *Id.* at 586-87.

152. *Id.* at 592.

153. *Id.*

154. *Id.* at 601.

155. *Herrick v. Grindr, LLC*, No. 18-396 (2d Cir. Mar. 27, 2019).

156. *Herrick v. Grindr, LLC*, 140 S. Ct. 221 (2019).

157. *Malwarebytes v. Enigma Software Grp.*, 141 S. Ct. \*13, \*18 (2020) (Thomas, J., concurring in denial of certiorari).

“It simply would give plaintiffs a chance to raise their claims in the first place.”<sup>158</sup>

It is unclear whether other Supreme Court Justices share Justice Thomas’s views on § 230. The Court’s denial of certiorari in *Herrick* and other § 230 cases suggests that the Supreme Court is not eager to wade into the statute any time soon.

In recent years, some federal appellate court judges have written individual concurrences and dissents in which they express frustration with the breadth of § 230’s protections. Perhaps the most notable example was a 2016 opinion affirming the § 230-based dismissal of sex trafficking-related claims against Backpage. The First Circuit concluded the opinion by noting the plaintiff’s argument that Backpage enabled sex trafficking. “But Congress did not sound an uncertain trumpet when it enacted the CDA, and it chose to grant broad protections to internet publishers,” Judge Selya wrote for the unanimous three-judge panel, which included retired Supreme Court Justice Souter. “Showing that a website operates through a meretricious business model is not enough to strip away those protections. If the evils that the appellants have identified are deemed to outweigh the First Amendment values that drive the CDA, the remedy is through legislation, not through litigation.”<sup>159</sup>

Congress responded within two years, passing the first ever substantive amendment to § 230, abrogating the immunity for some civil actions and state criminal prosecutions involving sex trafficking.<sup>160</sup> Congress has not amended § 230 since 2018, but other judges have called on legislators to consider changes to the statute.

Consider the late Judge Katzmann’s separate partial concurrence in a Second Circuit opinion that affirmed the § 230 dismissal of claims against Facebook that arose from its alleged violation of the Anti-Terrorism Act by provisioning a platform to Hamas and using “sophisticated algorithms” to present Hamas content to users.<sup>161</sup>

Section 230, Judge Katzmann wrote, does not necessarily apply to claims surrounding Facebook’s promotion of content.

“First, Facebook uses the algorithms to create and communicate its own message: that it thinks you, the reader—you, specifically—will like this

---

158. *Id.*

159. *Doe v. Backpage*, 817 F.3d 12 (1st Cir. 2016).

160. Allow States and Victims to Fight Online Sex Trafficking Act (“FOSTA”), Pub. L. No. 115-164, 132 Stat. 1253 (2018).

161. *Force v. Facebook, Inc.*, 934 F.3d 53, 77 (2d Cir. 2019) (Katzmann, J., partial concurrence and partial dissent).

content,” he wrote. “And second, Facebook’s suggestions contribute to the creation of real-world social networks. The result of at least some suggestions is not just that the user consumes a third party’s content.”<sup>162</sup>

Although § 230 protects Facebook for the publication of third-party content, Judge Katzmman reasoned, the statute does not protect it for claims arising from Facebook’s use of that content. This is in line with the approach of circumventing § 230 by arguing that the claims do not treat the platform as the publisher or speaker of third-party content. According to Katzmman, “it strains the English language to say that in targeting and recommending these writings to users—and thereby forging connections, developing new social networks—Facebook is acting as ‘the *publisher* of information provided by another information content provider.”<sup>163</sup>

Judge Katzmman concluded his opinion with a call for Congress to consider whether § 230 continues to serve the purposes for which it was passed in 1996. “The text and legislative history of the statute shout to the rafters Congress’s focus on reducing children’s access to adult material,” he wrote. “Congress could not have anticipated the pernicious spread of hate and violence that the rise of social media likely has since fomented. Nor could Congress have divined the role that social media providers themselves would play in this tale.”<sup>164</sup>

Judge Katzmman has not been the only judge to write a separate opinion urging a more modest interpretation of § 230. In a partial concurrence and partial dissent in a similar Anti-Terrorism Act case in 2021, Judge Gould of the Ninth Circuit also argued that § 230 does not apply to platforms’ use of algorithms.<sup>165</sup>

Largely echoing Katzmman’s partial dissent, in *Gonzalez v. Google*, Gould wrote that he would prefer for Congress and the executive branch to “seriously grapple” with the many social problems that arise from a lack of regulation of social media:

But if Congress continues to sleep at the switch of social media regulation in the face of courts broadening what appears to have been its initial and literal language and expressed intention under § 230, then it must fall to the federal courts to consider

---

162. *Id.* at 82

163. *Id.* at 76-77 (emphasis added) (quoting 47 U.S.C. § 230(c)(1)).

164. *Id.* at 88.

165. *Gonzalez v. Google, LLC*, 2 F.4th 871 (9th Cir. 2021), *reh’g en banc denied*, 21 F.4th 665 (9th Cir. 2022) (Gould, J., concurring).

rectifying those errors itself by providing remedies to those who are injured by dangerous and unreasonable conduct.<sup>166</sup>

Gould linked the lack of social media regulation to current political problems such as election misinformation, writing about concerns that social media platforms can “distort and tribalize public opinion, to spread falsehoods as well as truth, and to funnel like-minded news reports to groups in a way that makes them think there are ‘alternative facts’ or ‘competing realities’ that exist, rather than recognize more correctly that there are ‘truth’ and ‘lies.’”<sup>167</sup> In October 2022, the Supreme Court granted certiorari in *Gonzales*, marking the first time that the Court has agreed to interpret Section 230.

Even if the Supreme Court retains the broad *Zeran* precedent, Congress might narrow it. The separate opinions of Judge Gould and Judge Katzmann are not binding precedent, but they are remarkable in that federal judges are writing not only to state their interpretations of the law but to urge Congress to consider changing § 230. It remains to be seen whether their opinions will have the same impact as Judge Selya’s and cause Congress to further amend the law. But since 2019, members of Congress have introduced more than thirty-five bills that would either amend or repeal § 230.<sup>168</sup> Some bills aim to reduce the discretion that platforms have in blocking content and suspending users, such as by imposing viewpoint neutrality requirements on moderation.<sup>169</sup> Other bills impose a duty of care on platforms to encourage them to block harmful content more aggressively.<sup>170</sup> And some bills exempt from § 230’s protections particular types of harmful third-party content, such as civil rights violations and harassment.<sup>171</sup>

#### IV. PRINCIPLES FOR § 230 REFORM

Analyzing each of the proposed § 230 reform bills would be of limited use for a law review article, as the list of proposals likely will continue to grow and, as of the time of publication, no bill appears to be particularly likely to pass. Some bills carve out particular categories of claims from § 230 protection, others impose new procedural requirements on platforms, some restrict the

---

166. *Id.*

167. *Id.*

168. Meghan Anand, Kiran Jeevanjee, Daniel Johnson, Brian Lim, Irene Ly, Matt Perault, Jenna Ruddock, Tim Schmeling, Niharika Vatikonda, Noelle Wilson & Joyce Zhou, *All the Ways Congress Wants to Change Section 230*, SLATE (Feb. 11, 2022, 5:45 AM), <https://slate.com/technology/2021/03/section-230-reform-legislative-tracker.html>.

169. *Id.*

170. *Id.*

171. *Id.*



ability of platforms to moderate content, and others repeal the law entirely.<sup>172</sup> Indeed, with some bills aiming to reduce the amount of moderation that platforms perform and others seeking to increase the amount of moderation, it is hard to conceive of an easy consensus that addresses all concerns.

This Part will instead briefly suggest principles that Congress should keep in mind as it considers these proposals and develops new ones—or decides to refrain from § 230 changes. I do not suggest that Congress should carve § 230 into stone for eternity; it is a statute that Congress can and should assess regularly. But as this Part argues, § 230 changes cannot address every problem with the internet. Moreover, changes to the statute may have unintended consequences.

#### A. ELIMINATING § 230 WON'T ELIMINATE THE FIRST AMENDMENT

As the subsequently corrected *New York Times* headline about hate speech shows, commentators often blame § 230 for harmful speech that the First Amendment protects, no matter if § 230 is on the books. If Congress were to repeal § 230 tomorrow, it still could not constitutionally pass a law that holds platforms liable for online hate speech.<sup>173</sup> Nor could Congress pass a statute that imposes a blanket prohibition on platforms' distribution of disinformation, as the First Amendment protects many types of lies.<sup>174</sup>

The First Amendment not only prohibits the government from directly banning protected speech; it also prohibits the government from requiring platforms to ban that speech. As a corollary, the First Amendment does not prohibit platforms from independently deciding to block that same speech. This is due to the state action doctrine, the principle that the First Amendment generally only restricts the actions of the government and not the voluntary actions of private parties that do not involve government intervention.<sup>175</sup> As

---

172. For a good summary of the pending § 230 bills, see *id.* For an analysis of the different types of proposals, see Mark A. Lemley, *The Contradictions of Platform Regulation*, 1 J. FREE SPEECH L. 303 (2021).

173. See *Matal v. Tam*, 137 S. Ct. 1744, 1764 (2017) (“Speech that demeans on the basis of race, ethnicity, gender, religion, age, disability, or any other similar ground is hateful; but the proudest boast of our free speech jurisprudence is that we protect the freedom to express the thought that we hate.”) (internal quotation marks and citation omitted).

174. See *United States v. Alvarez*, 567 U.S. 709, 732 (2012) (plurality) (“The remedy for speech that is false is speech that is true. This is the ordinary course in a free society. The response to the unreasoned is the rational; to the uninformed, the enlightened; to the straightout lie, the simple truth.”).

175. See *Manhattan Comty. Access Corp. v. Halleck*, 139 S. Ct. 1921, 1925 (2019) (“The Free Speech Clause of the First Amendment constrains governmental actors and protects

Justice Kavanaugh wrote in 2019, only in “a few limited circumstances” can a private company be a state actor for First Amendment purposes: “(i) when the private entity performs a traditional, exclusive public function; (ii) when the government compels the private entity to take a particular action; or (iii) when the government acts jointly with the private entity.”<sup>176</sup>

Kavanaugh’s second exception could raise issues for government-imposed moderation mandates for platforms because a court likely would view any legal requirement to moderate as government compulsion. And the third exception makes it difficult for platforms to voluntarily partner with the government to identify and block harmful user content and actors, as such a partnership could be seen as a joint action with the government.

But when platforms independently and voluntarily adopt content moderation policies and procedures, the First Amendment does not constrain their decisions.<sup>177</sup> This freedom from the First Amendment’s constraints has enabled platforms to ban constitutionally protected content such as hate speech and misinformation.

Section 230 helps provide the platforms with this flexibility. Section 230(c)(2) explicitly provides immunity for good-faith efforts to block objectionable content, but the First Amendment also protects such editorial discretion.<sup>178</sup> Section 230(c)(1) has perhaps been even more important than § 230(c)(2) in providing platforms with the breathing space to moderate constitutionally protected content. Although the First Amendment protects the platforms’ ability to moderate this content, § 230(c)(1) has precluded more courts from adopting the *Stratton Oakmont* rule and holding platforms liable for all user content that they leave up just because they have moderated some content. To be sure, there is a strong argument that *Stratton Oakmont*

---

private actors. To draw the line between governmental and private, this Court applies what is known as the state-action doctrine.”).

176. *Id.* at 1928 (cleaned up).

177. *See* *Prager Univ. v. Google, LLC*, 951 F.3d 991, 994 (9th Cir. 2020) (“Despite YouTube’s ubiquity and its role as a public-facing platform, it remains a private forum, not a public forum subject to judicial scrutiny under the First Amendment.”); *Howard v. America Online*, 208 F.3d 741, 754 (9th Cir. 2000) (“There is nothing in the record that supports the contention that AOL should be considered a state actor.”).

178. *See* *Miami Herald Publ’g v. Tornillo*, 418 U.S. 241, 258 (1974) (“The choice of material to go into a newspaper, and the decisions made as to limitations on the size and content of the paper, and treatment of public issues and public officials—whether fair or unfair—constitute the exercise of editorial control and judgment. It has yet to be demonstrated how governmental regulation of this crucial process can be exercised consistent with First Amendment guarantees of a free press as they have evolved to this time.”).

misinterpreted the common law of distributor liability,<sup>179</sup> but few other cases interpret this area of the law as applied to the internet.

If Congress amends § 230, it should ensure that it does not recreate the perverse incentive of *Stratton Oakmont*. Eliminating § 230(c)(1) entirely runs the risk of such an outcome. A slightly narrower amendment, dictating that online services are the distributors but not the publishers of third-party content, could help to avoid a *Stratton Oakmont* outcome. Yet as the next Section argues, even this semi-repeal of § 230(c)(1) could have substantial unintended consequences.

## B. § 230 PROVIDES CERTAINTY TO PLATFORMS

Imagine if Congress did, in fact, amend § 230 to impose distributor liability on all online platforms.<sup>180</sup> Or, absent an amendment, the Supreme Court could follow Justice Thomas's lead and reject *Zeran*, leading to the same outcome.

We cannot say precisely what a distributor liability regime would look like for online platforms. Section 230's existence since the dawn of the modern internet has obviated the need for courts to apply common law distributor liability standards to online platforms. If platforms were considered distributors, they would face liability if they (1) knew or (2) had reason to know of defamatory or otherwise unlawful user content.

What does it mean for a platform to “know” about defamatory or unlawful user content? At the very least, the platform could face liability if it had actual knowledge of the content. Under *Hamling*, liability would not hinge on the platform's knowledge that the content was illegal; merely knowing about the particular content would suffice.<sup>181</sup> Such a standard could create a notice-and-takedown regime under which an aggrieved party could establish the platform's “knowledge” by notifying the platform. For instance, consider a restaurant that is unhappy with a Yelp review claiming that the chicken it served was partly raw. If the restaurant complained to Yelp that the review was inaccurate, the restaurant could then argue that Yelp had knowledge of the allegedly defamatory review. Yelp would then face the prospect of defending a defamation suit on the merits in court. Yelp likely cannot afford to investigate whether the restaurant actually served raw chicken, so its most prudent response would be to remove the review.

---

179. See Mike Godwin, CYBER RIGHTS: DEFENDING FREE SPEECH IN THE DIGITAL AGE 97 (2003) (“Logically, Justice Ain's interpretation of *Cubby v. CompuServe* makes no sense.”).

180. See H.R. 2000, 117th Cong. (2021) (stating that Section 230 shall not “be construed to prevent a provider or user of an interactive computer service from being treated as the distributor of information provided by another information content provider”).

181. See *supra* Section II.A.

But under the common law, distributors also face liability if they had “reason to know” of the defamatory or unlawful content. The courts have not explained when a distributor has a “reason to know” of user content but, by its very terms, it encompasses a broader range of scenarios than actual knowledge. Shortly after § 230 was passed in 1996—when it appeared that the statute merely overruled *Stratton Oakmont*—Floyd Abrams wrote an article that warned of the uncertainty created by imposing liability if an online service had ‘reason to know’ of the user content.

“Is this a negligence standard underprotective of on-line providers and their First Amendment rights?” Abrams wrote. “It sure sounds a lot less protective than *New York Times v. Sullivan*, which is the opposite of ‘reason to know’ and applies a standard of actual knowledge or actual serious doubts as to truth or falsity.”<sup>182</sup>

Because the Fourth Circuit issued *Zeran* the next year, Abrams’s concerns about distributor liability for online platforms remained hypothetical. *Zeran*—and its widespread adoption by courts nationwide—meant that whether a platform knew or had reason to know of particular user content was irrelevant for liability purposes.

A repeal of or substantial amendment to § 230 could bring back the uncertainty that Abrams highlighted in 1996. Social media providers, consumer review sites, community bulletin boards, and other platforms would scramble to determine when they know or have reason to know of user content. Smaller platforms with limited legal resources might decide to eliminate venues for user-generated content.

Unless courts provide sufficient certainty about the protections that platforms receive under a distributor liability regime, a rational platform would err on the side of taking down user content that might be defamatory or otherwise lead to potential liability. At the very least, distributor liability would create a notice-and-takedown system, allowing aggrieved individuals to pressure platforms to take down user content. But platforms might be even more risk averse due to the vague “reason to know” standard and proactively remove controversial content even without receiving a complaint.

To some critics of § 230—particularly those who believe that platforms do not adequately moderate harmful content—this very well may be a welcome change. Under a distributor liability system, platforms would have a substantial incentive to block harmful content. The downside is that they also would block content that is not necessarily harmful or illegal; overfiltering is a given when

---

182. Floyd Abrams, *First Amendment Postcards from the Edge of Cyberspace*, 11 ST. JOHN’S J. LEGAL COMMENT 693, 704 (1996).

moderating content at scale (and, as described in Section IV.D of this Article, there often is not a “correct” decision about moderation). The § 230 critics who believe that platforms already block too much user content would be particularly disappointed by a distributor liability system as risk-averse platforms would block more content than they otherwise would with the full § 230 protections in place. Indeed, the notice-and-takedown regime for copyright claims under § 512 of the Digital Millennium Copyright Act has resulted in platforms often being risk averse and taking down disputed user content to avoid liability.<sup>183</sup>

### C. § 230 CARVEOUTS CAN HAVE SWEEPING IMPACTS

Not all § 230 reform proposals would entirely remove the statute’s broad protections for platforms. Some proposals would retain the core protections of § 230(c)(1) but exempt particular types of claims. For instance, the Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms Act, introduced in the Senate in February 2021, would remove § 230 protections for claims involving civil rights, antitrust, stalking, harassment, intimidation, international human rights law, and wrongful death.<sup>184</sup> The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act, introduced in 2020, would remove § 230 protections for certain civil claims and state criminal prosecutions involving child sex abuse material.<sup>185</sup>

Carve-outs to § 230 are an attractive alternative to complete overhauls or repeals of liability protection. The categories of content described above are harmful and often deplorable. The challenge, however, is to avoid incentives for platforms to overcensor content that does not fall within those categories.

Like all businesses, platforms have lawyers. And lawyers are understandably risk averse, particularly when the liability rules are unclear. If Congress changes the law to impose more potential liability for particular types of content, platforms likely will more aggressively moderate not only the content that is clearly illegal but other user content that could possibly fall within that category. Even if it is unclear whether the § 230 exception would

---

183. See Corynne McSherry, *Platform Censorship: Lessons from the Copyright Wars* ELECTRONIC FRONTIER FOUNDATION (Sept. 26, 2018), <https://www EFF.ORG/deeplinks/2018/09/platform-censorship-lessons-copyright-wars> (“Many takedowns target clearly infringing content. But there is ample evidence that rightsholders and others abuse this power on a regular basis—either deliberately or because they have not bothered to learn enough about copyright law to determine whether the content to which they object is actually unlawful.”).

184. S. 299, 117th Cong. § 2 (2021).

185. S. 3398.

apply, or whether the platform would face liability without § 230 protection, the platform would likely avoid risking the cost of litigating a case on the merits.

The only significant amendment to § 230 provides a case study as to how platforms react to new § 230 exceptions. The 2018 sex trafficking law, the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA),<sup>186</sup> created new exceptions to § 230 for civil claims under a federal sex trafficking law and state criminal prosecutions would constitute violations of certain federal criminal laws regarding sex trafficking and the promotion or facilitation of prostitution.<sup>187</sup>

Within days of FOSTA's passage, online classified ad site Craigslist removed its entire personal ad section. "Any tool or service can be misused," the site wrote. "We can't take such risk without jeopardizing all our other services, so we have regrettably taken craigslist personals offline. Hopefully we can bring them back some day."<sup>188</sup> Personals ads serve a wide range of lawful purposes. But because they potentially could be misused by sex traffickers—and the scope of liability under FOSTA was unknown—Craigslist made the risk-based decision to remove the entire personals ads section.

FOSTA's enactment—along with the FBI's seizure of Backpage a few days before FOSTA was signed into law<sup>189</sup>—reduced the availability of platforms for sex workers. The lack of online platforms has reportedly driven many sex workers to bars or streets, increasing the danger that they face.<sup>190</sup> After conducting an online survey of ninety-eight sex workers, Danielle Blunt and Ariel Wolf concluded that FOSTA "has created an environment where marginalised populations are pushed into increased financial insecurity, which, in turn, makes them more vulnerable to labour exploitation and trafficking in the sex industry."<sup>191</sup> A 2021 *Columbia Human Rights Law Review* article summarized the impacts of FOSTA:

---

186. Allow States and Victims to Fight Online Sex Trafficking Act ("FOSTA"), Pub. L. No. 115-164, 132 Stat. 1253 (2018).

187. *Id.*

188. FOSTA, CRAIGSLIST, <https://www.craigslist.org/about/FOSTA> (last visited May 16, 2022).

189. Daniel Oberhaus, *The FBI Just Seized Backpage.com*, VICE (Apr. 6, 2018).

190. See Dean DeChiaro, *Sex Workers, Sidelined in Last Section 230 Debate, Seek a Seat at the Table*, ROLL CALL (Feb. 23, 2021), <https://rollcall.com/2021/02/23/sex-workers-sidelined-in-last-section-230-debate-seek-a-seat-at-the-table/>.

191. Danielle Blunt & Ariel Wolf, *Erased: The Impact of FOSTA-SESTA and the Removal of Backpage on Sex Workers*, 14 ANTI-TRAFFICKING R. 117 (2020).

The result is that people in the sex trades, who work in legal, semi-legal, and criminalized industries, have been forced into dangerous and potentially life-threatening scenarios. Many no longer have access to affordable methods of advertising and have returned to outdoor work or to in-person client-seeking in bars and clubs, where screening of the type that occurs online is impossible, and where workers are more vulnerable to both clients and law enforcement. These effects have been most impactful on sex workers facing multiple forms of marginalization, including Black, brown, and Indigenous workers, trans workers, and workers from lower socio-economic classes, who are prohibited from or unable to access more expensive advertising sites that may not be as impacted by FOSTA.<sup>192</sup>

FOSTA was a well-intentioned amendment to § 230 that sought to address the very real problem of sex trafficking. It is unclear whether FOSTA actually reduced sex trafficking, as other means are available to sex traffickers besides public-facing websites that are most likely to care about § 230. But we do know that FOSTA's impacts reached far beyond sex trafficking and that platforms' reactions to the increased liability has made life more dangerous for sex workers.

The fallout from FOSTA suggests that platforms will react quickly and in a risk-averse manner to new § 230 exceptions. Given the uncertainty created by the new potential liability, many platforms likely will block content that might even possibly fall within the exception. Accordingly, Congress should create new § 230 carveouts with great care, conscious of the unintended consequences of the new liability.

#### D. "NEUTRALITY" IS ELUSIVE

Other § 230 proposals seek to limit platforms' ability to moderate user content. These bills often stem from concerns that platforms are politically biased and unequally censor certain political views (often those of conservatives). For instance, the Protecting Constitutional Rights from Online Platform Censorship Act, introduced in the House in January 2021, would prohibit platforms from taking "any action to restrict access to or the availability of" First Amendment-protected user content."<sup>193</sup> The Stop Suppressing Speech Act, introduced in October 2020, would amend

---

192. Kendra Albert, Elizabeth Brundige & Lorelei Lee, *FOSTA in Legal Context*, 52 COLUM. HUM. RTS. L. REV. 1084, 1089-90 (2021).

193. H.R. 83, 117th Cong. (2021).

§ 230(c)(2) so that it only applies to a narrower category of user content, including that which promotes violence or terrorism.<sup>194</sup>

The proposals often stem from a common misrepresentation that § 230 only applies to “neutral platforms.”<sup>195</sup> As explained in Part I.B, Congress passed § 230 to overturn the perverse incentives created by *Stratton Oakmont* and provide platforms with the flexibility to moderate user content without suddenly becoming liable for everything on their sites.<sup>196</sup> Some critics who acknowledge that § 230 does not require neutrality argue that it should do so, and they suggest amending the law to impose a neutrality or common carriage requirement.<sup>197</sup>

From their perspective, § 230 provides online platforms with protection that goes beyond that of the First Amendment—protection that offline media do not enjoy. If platforms receive § 230 protection, they argue, the platforms should not moderate in a biased manner. Although the desire for “neutral platforms” might be understandable, on closer review it is impossible to achieve (and even if it were possible, it would not be desirable).

To see why, begin with a simple question: What does it mean for a platform to be neutral? Does it mean that the platform should not engage in any moderation at all? Such a policy could result in a torrent of harmful and illegal content. For instance, in the first quarter of 2021, Facebook took action on five million pieces of content that violated its child nudity and sexual exploitation policies.<sup>198</sup> Few people would argue that such content should remain on a public platform.

---

194. S. 4828, 116th Cong. (2020).

195. See Catherine Padhi, *Ted Cruz vs. Section 230: Misrepresenting the Communications Decency Act*, LAWFARE (Apr. 20, 2018), <https://www.lawfareblog.com/ted-cruz-vs-section-230-misrepresenting-communications-decency-act> (quoting Sen. Ted Cruz as saying to Facebook CEO Mark Zuckerberg, “The predicate for Section 230 immunity under the CDA is that you’re a neutral public forum. Do you consider yourself a neutral public forum, or are you engaged in political speech, which is your right under the First Amendment.”).

196. See Adi Robertson, *Why the Internet’s Most Important Law Exists and How People Are Still Getting It Wrong*, THE VERGE (June 21, 2019) (“They wanted platforms to feel free to make these judgments without risking the liability that Prodigy faced.”).

197. See, e.g., Adam Candeub, *Bargaining for Free Speech: Common Carriage, Network Neutrality, and Section 230*, 22 YALE J.L. TECH. 391, 433 (2020) (“These reforms would include an antidiscrimination requirement or requirements that dominant platforms share blocking technologies with users so that individuals, not corporate platforms, set the boundaries of on-line speech.”).

198. See *Community Standards Enforcement Report*, META (2021), <https://transparency.fb.com/data/community-standards-enforcement/child-nudity-and-sexual-exploitation/facebook/>.



A slightly more refined version of the neutrality argument is that platforms should only receive § 230 protections if they allow all constitutionally protected content on their services. Because child sex abuse material is categorically not constitutionally protected such a requirement would still permit a platform to block that content. But platforms also moderate a great deal of content that many would agree should be blocked. Would content that qualifies as commercial speech for First Amendment analysis be covered by a neutrality requirement? For instance, Facebook in the first quarter of 2021 took action on 905 million pieces of content that violated its spam policies.<sup>199</sup> Few would argue that the internet would benefit from more spam.

Another version of the neutrality argument is that platforms should be permitted to moderate content—even content that is constitutionally protected—provided that the platforms engage moderate in a “viewpoint neutral” manner. Although that sounds slightly more reasonable, it also is difficult to conceive of how such a policy would work in practice. For instance, in the first quarter of 2021, Facebook took action on about 25 million pieces of content under its hate speech policy.<sup>200</sup> Facebook’s detailed hate speech policy contains a long list of the types of attacks on individuals prohibited on the platform.<sup>201</sup> Online political arguments can get heated, and often include hateful remarks. The decision to include or exclude a particular type of speech within the definition of hate speech might be seen as politically biased. Depending on how it is drafted, a viewpoint neutrality requirement might preclude a platform from banning hate speech and other constitutionally protected content.

Content moderation is difficult, particularly when dealing with up to thousands of pieces of user content a second. Setting policies and identifying content that violates those policies is a tall task, and it is impossible to satisfy everyone, in part because users have different expectations and understandings of what kind of content is harmful. Consider the coronavirus pandemic. In 2020, the theory that COVID-19 originated from a lab in China was largely criticized. But in 2021, more mainstream commentators and politicians began to find the theory at least plausible. Should a social media site have classified the lab leak theory as misinformation in 2020 and taken down any posts containing it? What about in 2021? Or should the platforms have been *required* to carry the theory in 2021, under the assumption that the platforms must be “neutral?” What about in 2020? All of these questions are hard, and the system

---

199. *Id.*

200. *Id.*

201. *Hate Speech*, META <https://transparency.fb.com/de-de/policies/community-standards/hate-speech/> (last visited May 18, 2022).

under § 230 and the First Amendment provides platforms with the flexibility to make these decisions.

Indeed, § 230 is very much a free market-based law that assumes that by providing platforms with the breathing room to set their own policies, they will best meet the demands of many of their users. If platforms are too restrictive or not restrictive enough, at least according to the theory, users will migrate to another platform. Of course, this market-based theory may not function smoothly if there is not sufficient competition for the largest platforms. But imposing a neutrality requirement would not necessarily solve this problem, as it would overwhelm platforms with content that makes the overall user experience less pleasant, and in some cases, more dangerous.

In short, “neutral platforms” is a tempting proposition. But a world in which platforms were entirely neutral would have sweeping negative consequences for the internet, causing it to be filled with spam, illegal images, violence, and so many other things that most users would expect platforms to block. A modified version of neutrality might avoid some of the worst outcomes, but it is difficult to imagine consensus on a more flexible view of “neutrality.”

#### E. TRANSPARENCY COULD IMPROVE THE § 230 DEBATE

Much of the § 230 debate has been driven by widespread misunderstandings—innocent or otherwise. Some of these misunderstandings involve easily corrected legal errors. No, § 230 does not require neutrality.<sup>202</sup> No, repealing § 230 would not suddenly create a cause of action for

---

202. Catherine Padhi, *Ted Cruz vs. Section 230: Misrepresenting the Communications Decency Act*, LAWFARE (Apr. 20, 2018, 10:00 AM), <https://www.lawfareblog.com/ted-cruz-vs-section-230-misrepresenting-communications-decency-act> (“Sen. Ted Cruz, the Republican from Texas, suggested as much while questioning Facebook CEO Mark Zuckerberg during last week’s congressional hearings. But Cruz’s representation of Section 230 is misleading. There is no requirement that a platform remain neutral in order to maintain Section 230 immunity. And Facebook does not have to choose between the protections of Section 230 and those of the First Amendment; it can have both.”).

constitutionally protected speech.<sup>203</sup> No, § 230 does not apply to copyright infringement claims.<sup>204</sup>

But other misunderstandings come from the complex nature of moderating content at scale. Under § 230's protections, platforms have voluntarily developed detailed policies and procedures for constitutionally protected but objectionable user content. The policies are not merely choices of whether to take down or leave up content; they have a long menu of options that they believe are in the best interests of their users (and their businesses). Eric Goldman has documented the wide range of remedies beyond takedowns. They include relocating content, suspending accounts, using credibility badges, demonetizing content, educating users, and reducing service levels.<sup>205</sup>

Goldman's work is part of a growing body of scholarship that has begun to provide some transparency as to how platforms moderate content at scale. Sarah Roberts has documented the lives of the workers who moderate the content for social media companies.<sup>206</sup> Kate Klonick has traced the history of the earliest social media content moderation policies<sup>207</sup> and the development of the Facebook Oversight Board.<sup>208</sup> And evelyn douek has explained the role of international human rights law in content moderation.<sup>209</sup> More than a decade ago, Danielle Citron highlighted the persistent harassment that people face online and proposed solutions.<sup>210</sup> These works demonstrate the nuances and complexities of content moderation. Unfortunately, this scholarship has

---

203. Betsy Klein, White House reviewing Section 230 amid efforts to push social media giants to crack down on misinformation, CNN (July 20, 2021) ("The Section 230 debate is taking on new urgency in recent days as the administration has called on social media platforms to take a more aggressive stance on combating misinformation. The federal law, which is part of the Communications Decency Act, provides legal immunity to websites that moderate user-generated content.").

204. See Andrew Marantz, *Free Speech is Killing Us*, N.Y. Times (Oct. 4, 2019) <https://www.nytimes.com/2019/10/04/opinion/sunday/free-speech-social-media-violence.html> (correcting opinion piece to state that "[a]n earlier version of this article misidentified the law containing a provision providing safe haven to social media platforms. It is the Communications Decency Act, not the Digital Millennium Copyright Act.").

205. Eric Goldman, *Content Moderation Remedies*, 28 MICH. TECH. L. R. 1 (2021).

206. Sarah Roberts, BEHIND THE SCREEN: CONTENT MODERATION IN THE SHADOWS OF SOCIAL MEDIA (2019).

207. Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2018).

208. Kate Klonick, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression*, 129 YALE L. J. 2232 (2020).

209. evelyn douek, *The Limits of International Law in Content Moderation*, 6 UCI J. OF INT'L, TRANSNATIONAL, AND COMP. L. 37 (2021).

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

not fully informed the debate in the popular media and Congress, where misconceptions continue to proliferate.

To address this knowledge gap, Congress should consider forming a nonpartisan commission of experts to gather facts about how content moderation currently works, what is possible, and how changes in the law might positively or negatively affect the field. As I wrote in a 2019 proposal for such a commission, other congressional commissions in areas such as national security and cybersecurity have helped to develop informed records and thoughtful proposals.<sup>211</sup> As one example, the 2020 defense authorization bill contained twenty-five recommendations from the Cyberspace Solarium Commission, which Congress had formed to gather facts and shape policy about emerging cyber threats.<sup>212</sup>

A nonpartisan content moderation commission would be an alternative to the current discourse around § 230, which has seen dozens of conflicting proposals but very few facts about how content moderation actually works and how these bills would change the system. As seen with FOSTA, even a change to one narrow area of user content can have substantial effects on platforms' behavior.

Transparency also can come from the platforms. Many large and small platforms publicly post user content policies with varying degrees of detail. Some platforms, such as Facebook and Google, also publish transparency reports that at least provide some statistics about the content that they have removed. This is a good first step, and Congress should consider ways to better foster this transparency. For instance, the Platform Accountability and Consumer Transparency Act,<sup>213</sup> introduced in 2020 and 2021, would, among other things, require platforms to publish content moderation statistics and accessible content moderation policies. Platforms still would have the flexibility to establish moderation practices that they believe their users demand, but a transparency requirement would better inform their users and help § 230's market-based system function more efficiently. Even these more modest proposals would need close examination for First Amendment concerns. For instance, could a law require a newspaper to disclose how and

---

211. Jeff Kosseff, *Understand the Internet's Most Important Law Before Changing It*, REG. REV. (Oct. 10, 2019).

212. See Press Release, Cyberspace Solarium Commission, *NDAA Enacts 25 Recommendations from the Bipartisan Cyberspace Solarium Commission* (Jan. 2, 2021).

213. Platform Accountability and Consumer Transparency Act, S. 4066, 116th Cong. (2020).

why it decides which letters to publish or how it edits stories?<sup>214</sup> If not, conditioning § 230 protections on such transparency also could raise constitutional concerns.<sup>215</sup>

## V. CONCLUSION

This Article has sought to provide some clarity to the increasingly heated debate surrounding § 230. Understanding § 230's history, purpose, and mechanics is crucial in debating its future. This Article has a cautionary tone and explains how even minor changes to § 230 could have substantial (and perhaps unintended) consequences on content moderation and the everyday internet experience. The intention is not to suggest that Congress should avoid making any changes to § 230. No law is perfect, and the internet that Section 230 has shaped also is far from ideal. But our dissatisfaction with the current state of the internet is not a valid excuse for making sweeping changes to a fundamental internet law without fully considering the impacts that those changes would have. This Article has sought to inform what hopefully will be a more substantive and reality-based debate about the future of § 230 and online platforms.

---

214. See Eric Goldman, *Comments on the Platform Accountability and Consumer Transparency Act (the "PACT Act")* (July 27, 2020), <https://blog.ericgoldman.org/archives/2020/07/comments-on-the-platform-accountability-and-consumer-transparency-act-the-pact-act.htm>.

215. See *Elrod v. Burns*, 427 U.S. 347, 361 (1976) ("The denial of a public benefit may not be used by the government for the purpose of creating an incentive enabling it to achieve what it may not command directly.").

