COMMENTS

THE PRICE OF PROTECTION: HOW SECTION 230'S IMMUNITY FOR ONLINE PROVIDERS IMPEDES CALIFORNIA LEGISLATION DESIGNED TO ADDRESS CSAM*

I. INTRODUCTION

In 2021, the National Center for Missing and Exploited Children (NCMEC) reported that it had received more than thirty-five million images and videos to review for child sexual abuse material (CSAM).[1] CSAM is typically known in the legal system as child pornography.[2] However, organizations such as the NCMEC and the U.S. Department of Justice now prefer the label CSAM over child pornography because it shifts the focus to the impact sexual abuse and exploitation has on child victims.[3] When CSAM is posted on the internet, it poses the risk of continuously retraumatizing victims, because it remains available for anyone to access.[4] In addition to the permanence of CSAM, internet platforms have increased access to CSAM by allowing users to find and share the material at a massive scale.[5] Even more troubling, artificial intelligence now

---

* Alyssa Humeston, J.D. Candidate, Temple University Beasley School of Law, 2026. Thank you to my faculty advisor, Professor Laura Bingham, for her time and insight throughout the process. I am grateful for all the members of the *Temple Law Review* for their diligent work in preparing this piece for publication. Thank you to my friends for their unwavering support and for always knowing how to lift my spirits. Most of all, thank you to my wife, Andrea, who listened to every idea and encouraged me every step of the way.

1. U.S. DEP'T OF JUST., CHILD SEXUAL ABUSE MATERIAL 2 (2022), https://www.justice.gov/d9/2023-06/child_sexual_abuse_material_2.pdf [https://perma.cc/TB6P-J8CN].

2. 18 U.S.C. § 2256(8) (defining child pornography as "any visual depiction . . . of sexually explicit conduct, where—(A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct").

3. *Child Sexual Abuse Material*, NAT'L CTR. FOR MISSING & EXPLOITED CHILD., https://www.missingkids.org/theissues/csam [https://perma.cc/N5Q6-BJ3R] (last visited Oct. 20, 2025); U.S. DEP'T OF JUST., *supra* note 1, at 1 (noting that an international group focused on addressing child exploitation has also "formally recognized 'child sexual abuse material' as the preferred term").

4. *See Child Sexual Abuse Material*, *supra* note 3 ("In a recent survey led by the Canadian Centre for Child Protection, 67% of CSAM survivors said the distribution of their images impacts them differently than the hands-on abuse they suffered because the distribution never ends and the images are permanent.").

5. *Id.* ("The disturbing reality is that the internet platforms we use every day to connect with each other and share information, including social media, online gaming, and e-mail, are now being used to disseminate and collect CSAM.").

poses a new threat as the technology has been used to create CSAM.[6] All of this raises an important question: What remedies do victims of CSAM have against the actors who were complicit in their abuse?

Individuals who participate in the production, distribution, or possession of CSAM can be held criminally or civilly liable.[7] However, there are fewer ways to hold online providers accountable for their role in facilitating and disseminating CSAM. This distinction is due to the judiciary's interpretation of Section 230 of the Communications Decency Act, which provides broad immunity to online providers.[8] Section 230 "gives online providers immunity from civil action and state and local criminal action for material on their platform created by a third-party,"[9] which safeguards online providers from liability for failure to remove CSAM.[10] Recently, however, California passed two laws that open new avenues for holding social media platforms liable: one for failing to remove CSAM and a second for contributing to the online exploitation of children.[11]

This Comment explores whether California's law is an effective way for victims of CSAM to hold online providers accountable or whether Section 230 limits the scope of this legislation by granting broad immunity to online providers. Additionally, this Comment considers whether the First Amendment right to freedom of speech bars California's statute on constitutional grounds. Section II dissects these questions. Part II.A begins with an overview of the creation of Section 230, focusing on the goals and purpose of the legislation. Next, Part II.A outlines both the limits of Section 230 immunity for online providers and when online providers can be held liable for online content. From there, it considers how Section 230 preempts states from passing legislation that contradicts the federal law. Part II.B discusses current challenges to Section 230's immunity provisions, including California's new law and calls at the state and federal levels to amend Section 230 directly. Part II.C considers the limitations the First Amendment imposes on legislation regulating online content.

Section III analyzes whether California's new methods for holding online providers liable overcome the immunity granted by Section 230. Part III.A argues that the first method of liability passed in California is unconstitutional. While the First Amendment does not preclude California from passing legislation to regulate online content, the first avenue of liability is expressly and impliedly preempted by Section 230. Conversely, Part III.B argues that the second avenue of liability against social media platforms that materially contribute to CSAM is not preempted by Section 230. Finally, Part III.C

---

6. *Artificial Intelligence (AI) and the Production of Child Sexual Abuse Imagery*, INTERNET WATCH FOUND., https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/ [https://perma.cc/MAE6-ME9D] (last visited Oct. 20, 2025) ("The Internet Watch Foundation (IWF) has identified a significant and growing threat where AI technology is being exploited to produce child sexual abuse material (CSAM). Our first report in October 2023 revealed the presence of over 20,000 AI-generated images on a dark web forum in one month where more than 3,000 depicted criminal child sexual abuse activities. Since then the issue has escalated and continues to evolve.").

7. *See, e.g.*, 18 U.S.C. §§ 2251–2252, 2255, 2259–2260.

8. *See, e.g.*, Ricci v. Teamsters Union Loc. 456, 781 F.3d 25, 28 (2d Cir. 2015); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003).

9. U.S. DEP'T OF JUST., *supra* note 1, at 9.

10. *See* 47 U.S.C. § 230.

11. CAL. CIV. CODE §§ 3273.66, 3345.1 (West 2025).

asserts that Congress should amend Section 230 to confront the growing issue of CSAM on online platforms and to allow legislation that addresses the issue, like California's, to fully function.

II. OVERVIEW

This Section explains the origins of Section 230 and the extent of immunity the statute provides to online providers. While immunity under Section 230 generally prohibits states from imposing liability to online providers, there are limited exceptions to this immunity.[12] Even though courts have interpreted Section 230 immunity broadly,[13] California has passed legislation that aims to hold social media companies liable for failing to remove CSAM or if they "knowingly facilitate, aid, or abet" the online commercial sexual exploitation of children.[14] California is not the only government entity concerned with CSAM hosted by online providers and the immunity Section 230 provides.[15] Multiple sessions of Congress, state legislators, and a former U.S. attorney general have all called for the amendment, or complete overhaul, of Section 230 to address CSAM.[16] In addition to triggering Section 230, laws that attempt to regulate online content, such as California's, also implicate the First Amendment.[17] These laws can be facially unconstitutional when they unduly burden constitutionally protected speech.[18]

A. Section 230

Amid the rapid commercialization of the internet at the end of the twentieth century,[19] the Communications Act of 1934 was amended by the enactment of the Communications Decency Act of 1996 (CDA).[20] While increasing public access to the internet offered many people around the world immense access to information and communication, there were concerns about how this powerful technology might be used.[21] Section 230 of the CDA reflects the generally positive outlook on the advancing technology, as Congress emphasized in the statutory text that the internet offers an "extraordinary" opportunity to advance education and information.[22] Additionally, Congress noted that the internet provides a space for political discourse, cultural development, and intellectual activity.[23] However, Section 230 also highlights

12. 47 U.S.C. § 230(e).

13. *See infra* Part II.A.

14. CIV. §§ 3273.66–3273.69, 3345.1.

15. *See infra* Part II.B.

16. *See infra* Part II.B.

17. *See infra* Part II.C.

18. *See, e.g.*, Reno v. ACLU, 521 U.S. 844, 874 (1997).

19. *See Birth of the Commercial Internet*, U.S. NAT'L SCI. FOUND., https://new.nsf.gov/impacts/internet [https://perma.cc/54EC-BSQA] (last visited Oct. 20, 2025) ("Commercial firms noted the popularity and effectiveness of the growing internet and began to build their own network infrastructure, eventually producing products that provided basic connectivity and internet services.").

20. Communications Decency Act, Pub. L. No. 104-104, § 509, 110 Stat. 56, 137–39 (1996).

21. *See* 141 CONG. REC. 22045 (1995) (statement of Rep. Christopher Cox).

22. 47 U.S.C. § 230(a)(1).

23. *Id.* § 230(a)(3).

Congress's concern with the availability of online offensive material to children and the complexities of balancing government regulation of these computer services.[24]

Section 230 provides online providers legal immunity for content posted by another user on their platform and for their choice to restrict content on their site.[25] However, Section 230 does include some explicit exceptions to this immunity in which online providers can be held liable for online content.[26] Despite these carveouts, courts have interpreted Section 230 immunity broadly.[27] This broad immunity for online providers is fortified by the fact that states are prohibited from passing laws that are impliedly or expressly preempted by Section 230.[28] However, online providers can still be liable when they make material contributions to content or when the tools provided to users are not "neutral."[29]

1. The Goals and Purpose of Section 230

The motivation for creating Section 230 arose after two decisions in New York—one federal and one in the state trial court—came to diametrically opposed conclusions on the liability of online providers.[30] In 1991, the District Court for the Southern District of New York concluded in *Cubby, Inc. v. CompuServe, Inc.* that CompuServe (a computer service company that provided users access to online forums and information) could not be held liable for distributing defamatory publications to its users.[31] The court explained that CompuServe was equal to a public library in terms of editorial control, and it would be infeasible to require computer databases to filter their large publication libraries.[32] Conversely, in the 1995 case *Stratton Oakmont, Inc. v. Prodigy Services Co.*, a New York trial court found that an online provider could be found liable for its users' posts when the provider had informed its users that their content would be screened.[33] Applying this, the court determined that the online provider, Prodigy, could be held liable for its "editorial control."[34] Because Prodigy was deleting some posts on its bulletin boards for offensive content, the court believed Prodigy was acting as a publisher rather than a distributor.[35]

The conflict between *Prodigy* and *CompuServe* disincentivized online providers from regulating the content on their sites.[36] In response, Section 230 served two

24. *See* 141 CONG. REC. 22044–45 (1995) (statement of Rep. Christopher Cox).

25. 47 U.S.C. § 230(c).

26. *Id.* § 230(e).

27. *E.g.*, Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003).

28. *See* 47 U.S.C. § 230(e)(3); Gade v. Nat'l Solid Wastes Mgmt. Ass'n, 505 U.S. 88, 98 (1992).

29. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1169 (9th Cir. 2008) (providing examples of when online providers are liable for materially contributing to user content and when online providers are not liable for giving users neutral tools to use).

30. 141 CONG. REC. 22045 (1995) (statement of Rep. Christopher Cox).

31. 776 F. Supp. 135, 140 (S.D.N.Y. 1991).

32. *Id.*

33. No. 31063/94, 1995 WL 323710, at *4 (N.Y. Sup. Ct. May 24, 1995), *superseded by statute*, 47 U.S.C. § 230.

34. *Id.*

35. *Id.*

36. 141 CONG. REC. 22047 (1995) (statement of Rep. Robert Goodlatte).

purposes: (1) to "protect computer Good Samaritans" and online providers from liability for screening offensive material, and (2) to establish as policy that the United States opposed government regulation of internet content.[37] By protecting online providers from liability, the proponents of Section 230 believed they could continue and encourage the "energetic technological revolution" and simultaneously keep children shielded from pornographic and offensive material.[38]

2. Defining the Scope of Section 230 Immunity

"Interactive computer service" and "information content provider" are defined in the statute.[39] An interactive computer service is an internet system that allows multiple users access to a server.[40] Courts have interpreted "interactive computer service" to be a relatively expansive term.[41] As defined by Section 230, an information content provider is a "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."[42] The definition and interpretation of these two terms prevent online service providers from being found liable for "traditional editorial functions," such as deciding to publish, remove, or alter content.[43] Generally, interactive computer services qualify for Section 230 immunity if they do not function as an information content provider.[44] In function, Section 230 treats interactive computer services under a different standard than other publishers of information like newspapers, magazines, television, and radio.[45] These other content providers can be held liable for publishing material that has been written and prepared by others.[46]

For the last three decades, Section 230 has offered broad immunity to online providers for tort claims.[47] This immunity for an "interactive computer service" is detailed in Section 230(c), "Protection for 'Good Samaritan' blocking and screening of offensive material."[48] Section 230(c)(1) states that "[n]o provider or user of an interactive computer service [can] be treated as the publisher or speaker" of another "information content provider."[49] Section 230(c)(2) also states that providers of interactive computer services cannot be held liable for their choice to restrict obscene, violent, or objectionable material, or for allowing other information content providers to do so.[50]

---

37. *Id.* at 22045 (statement of Rep. Christopher Cox).

38. *Id.*

39. 47 U.S.C. § 230(f).

40. *Id.* § 230(f)(2).

41. Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003).

42. 47 U.S.C. § 230(f)(3).

43. Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).

44. *Carafano*, 339 F.3d at 1123.

45. Blumenthal v. Drudge, 992 F. Supp. 44, 49 (D.D.C. 1998).

46. *Id.*

47. *See, e.g.*, Ricci v. Teamsters Union Loc. 456, 781 F.3d 25, 28 (2d Cir. 2015); *Carafano*, 339 F.3d at 1123.

48. 47 U.S.C. § 230(c).

49. *Id.* § 230(c)(1).

50. *Id.* § 230(c)(2).

Section 230 also has exceptions to its immunity built into the statute.[51] Congress clarified that the statute has no effect on five specific types of federal and state law.[52] First, a person or entity can be liable for violating state laws that are consistent with Section 230.[53] Second, Section 230 has no effect on intellectual property law[54] nor, third, on specific electronic communications privacy laws.[55] Fourth, it does not restrict the enforcement of federal criminal laws, especially those relating to the distribution of harmful materials to minors for profit.[56] Finally, Section 230(e) outlines that the statute shall not interfere with federal criminal or civil law relating to the sex trafficking of minors or state and federal criminal law relating to the sex trafficking of minors and adults.[57]

This final exception was added through the enactment of the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA).[58] When FOSTA was passed in 2018, Congress noted that Section 230 was "never intended to provide legal protection to websites that unlawfully promote and facilitate prostitution and websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims."[59] Congress criticized websites for being "reckless" in allowing online sex trafficking to occur via their platforms and claimed the websites "have done nothing to prevent the trafficking of children and victims of force, fraud, and coercion."[60] FOSTA provides a route by which interactive computer services that intend to promote prostitution can be held criminally and civilly liable.[61]

The first federal court of appeals case to consider the extent of Section 230 immunity for online providers was the 1997 case, *Zeran v. America Online, Inc*.[62] In this defamation case, an individual, Zeran, sued America Online (AOL) for its delay in removing defamatory messages posted by another user and failing to filter other posts.[63] An unidentified user posted offensive messages on AOL's bulletin board and directed others to call Zeran's phone number.[64] Due to this post, Zeran began receiving death threats and other harassing phone calls.[65] When Zeran approached AOL and requested that it remove the bulletin post, AOL agreed to remove the content only for another advertisement to be posted the next day.[66]

---

51. Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 418 (1st Cir. 2007).

52. 47 U.S.C. § 230(e).

53. *Id.* § 230(e)(3).

54. *Id.* § 230(e)(2).

55. *Id.* § 230(e)(4).

56. *Id.* § 230(e)(1).

57. *See id.* § 230(e)(5).

58. Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (SESTA/FOSTA), sec. 4, § 230(e), 132 Stat. 1253, 1254 (2018).

59. *Id.* sec. 2, § 230, 132 Stat. at 1253.

60. *Id.*

61. *Id.* sec. 3, § 2421A, 132 Stat. at 1253–54.

62. 129 F.3d 327, 334 (4th Cir. 1997).

63. *Id.* at 328.

64. *Id.* at 329.

65. *Id.*

66. *Id.*

Zeran argued that interactive computer service providers could still be held liable despite Section 230 immunity when the provider fails to remove defamatory material after being given notice of the material's presence.[67] He argued that immunity under Section 230 eliminates only "publisher liability" and not "distributor liability."[68] Zeran noted that Congress used only the word "publisher" within the statute, which he believed displayed a desire to create publisher immunity and leave distributor liability intact.[69]

The Fourth Circuit quickly dismissed Zeran's argument and explained that distributor liability is merely a subset of publisher liability and therefore falls under the immunity provided by Section 230.[70] The court highlighted that communicating a defamatory statement and failing to remove a defamatory statement are both considered "publishing" that statement.[71] When online providers are given notice of content that should be removed, they are "thrust into the role of a traditional publisher."[72] In determining whether to publish or remove content, AOL and other online services are explicitly immune from liability for their role as the publisher of this content.[73] The Fourth Circuit reasoned that imposing liability on online service providers after notice of defamatory content would "defeat the dual purposes" of Section 230[74] and lead to the same outcome as in *Prodigy*: Online service providers would be incentivized to avoid regulation.[75]

In its opinion, the Fourth Circuit also recognized the infeasibility of subjecting online service providers to distributor liability.[76] The number of users on these online platforms, and the subsequent number of posts, would "create an impossible [regulatory] burden" on online service providers.[77] The court noted that every notice of a defamatory statement by a user would require the online service to investigate the post, conduct a legal analysis of the defamation claim, and make an editorial decision.[78] This three-step process would in effect encourage online service providers to remove content when notified regardless of whether the material was actually defamatory since the providers would be liable only for the publication of information.[79] The court noted that this would have a "chilling effect" on freedom of speech over the internet.[80] The Fourth Circuit affirmed the lower court's granting of summary judgment in favor of AOL after

67. *Id.* at 328.

68. *Id.* at 331.

69. *Id.* at 332.

70. *Id.*

71. *Id.*

72. *Id.*

73. *Id.* at 333.

74. *Id.* at 330, 333 ("Section 230 was enacted . . . [(1)] to maintain the robust nature of Internet communication and . . . [(2)] to keep government interference in the medium to a minimum.").

75. *Id.* at 331.

76. *Id.* at 333.

77. *Id.*

78. *Id.*

79. *Id.*

80. *Id.*

emphasizing that Section 230 "plainly immunizes" computer service providers from liability for content posted by third parties.[81]

3. Material Contribution and Neutral Tools

The key question in determining liability under Section 230 for online providers is whether the online provider can be treated as an information content provider.[82] As highlighted in *Zeran*, online providers can make some edits to third-party content without being considered the content provider.[83] The federal circuit courts have developed two tests to determine whether an online provider should be treated as an information content provider: the material contribution test and the neutral tools test.[84]

In 2008, the Ninth Circuit outlined these two tests in *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC* to determine a party's role in the "creation or development" of content.[85] The online service provider in that case, Roommates.com, was sued in federal court by the Fair Housing Council of San Fernando Valley and the City of San Diego for alleged violations of the Fair Housing Act and state discrimination laws.[86] To search housing listings or make posts on the website, Roommates.com required users to disclose their sex, sexual orientation, and family status.[87] Users also had to choose their preference for roommates based on the same three criteria.[88] Roommates.com then created profiles for these users that displayed their personal information and roommate preferences to other users.[89] Because of these requirements for use, the housing councils argued Roommates.com unlawfully displayed their users' discriminatory preferences.[90]

The Ninth Circuit explained that Section 230 immunity applies only if the online provider is not also an information content provider,[91] which is a party "responsible, in whole or in part, for the creation or development" of the content.[92] If an online provider passively displays another user's content to its users, then it is only a service provider.[93] But if the online provider creates its own content or is "responsible, in whole or in part" for creating content, the online provider is considered an information content provider as well.[94]

Because Roommates.com provided its users with a limited selection of answers for their housing preferences, the court determined that the online provider was also

81. *Id.* at 328.

82. *See* 47 U.S.C. § 230(c), (f)(3).

83. *Zeran*, 129 F.3d at 330.

84. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1169 (9th Cir. 2008).

85. *See id.* at 1163, 1169 (quoting 47 U.S.C. § 230(f)(3)).

86. *Id.* at 1162.

87. *Id.* at 1161.

88. *Id.*

89. *Id.* at 1161–62.

90. *Id.* at 1165.

91. *Id.* at 1162.

92. 47 U.S.C. § 230(f)(3).

93. *Roommates.com*, 521 F.3d at 1162.

94. *Id.* (quoting 47 U.S.C. § 230(f)(3)).

functioning as an information content provider.[95] Roommates.com acted as more than a passive transmitter of information in this situation, since its provided selection of answers contributed in part to the content.[96] Roommates.com became a developer of the information since it required users to "provide the information as a condition of accessing its service" and provided "a limited set of pre-populated answers."[97] Thus, the users and Roommates.com "collaborated" on each profile page.[98] The Ninth Circuit determined that Roommates.com could be held liable for asking discriminatory questions and using its users' answers to limit housing.[99]

The Ninth Circuit in *Roommates.com* found that a material contribution by an online service provider can be considered "development" under Section 230(f)(3) and, consequently, the service provider can be considered an information content provider.[100] When an online service contributes materially to illegal content, it can be held liable for that content as an information content provider.[101] The court provided several examples of what does and does not equate to material contribution under the facts of *Roommates.com*.[102] Where an online service provides "neutral tools" to its users who then use those tools to carry out unlawful searches, this act does not amount to development.[103] For example, the court explained that if an individual user had used an online site and searched "white roommate," the online service would be immune under Section 230 since the service did not materially contribute to the development of the illicit conduct.[104] In another illustration, the court claimed that if a dating site required users to input their demographic information with drop-down options and allowed users to search through other users based on this information, the website would maintain its immunity since it did not contribute to any illegal conduct.[105]

Additionally, an online provider retains Section 230 immunity where it edits user-created content that is unrelated to the illegal conduct, such as "correcting spelling, removing obscenity or trimming for length."[106] However, an online provider loses Section 230 immunity where it edits user material and the edits contribute to the illegal conduct.[107] For example, if an online provider removed the word "not" from a user's content reading "[John Doe] did *not* steal the artwork" and transformed the message into libel, it would be directly involved in the illegal conduct.[108] Under the facts of

95. *Id.* at 1166.
96. *Id.*
97. *Id.*
98. *Id.* at 1167.
99. *Id.*
100. *Id.* at 1167–68.
101. *Id.* at 1168.
102. *Id.* at 1169.
103. *Id.* (emphasis omitted).
104. *Id.*
105. *Id.*
106. *Id.*
107. *Id.*
108. *Id.*

Roommates.com, the online provider developed discriminatory questions, answers, and a search mechanism that were directly connected to the alleged illegality.[109]

The court concluded its opinion by highlighting that the outcome is consistent with the purpose of Section 230 and the intent of Congress.[110] Because Section 230 is an immunity statute, designed to "protect websites against the evil of liability for failure to remove offensive content," even in close cases where a plaintiff argues that the online provider "encouraged" illegality, that immunity should be enforced to protect the heart of Section 230 immunity.[111] The outcome protects the "free-flowing nature of [i]nternet speech and commerce," as intended by Congress when it enacted Section 230.[112] The Ninth Circuit emphasized that Congress intended to "encourage interactive computer services that provide users *neutral* tools to post content online" without fear of liability from content posted by third parties.[113]

Other circuits have since reaffirmed the distinction between neutral tools and material contribution that the Ninth Circuit provided in *Roommates.com*.[114] For example, in *FTC v. Accusearch, Inc.*, the Tenth Circuit held that the online provider, Accusearch, materially contributed to illegal activity on the site by encouraging its researchers to transform private information into a commodity.[115] Even though the information was posted by third parties on the website, Accusearch was responsible in part for the development of the content.[116] The online provider in *Accusearch* was not merely providing neutral tools, but its actions were aimed at generating unlawful content.[117]

Notably, in a more recent Ninth Circuit decision, the court reasoned that online providers are open to liability even when providing neutral tools.[118] In *Lemmon v. Snap, Inc.*, the parents of two boys brought suit against the social media provider, Snap, for its negligent design of a speedometer filter on the Snapchat application.[119] While providing neutral tools means that an online provider is not considered a creator or developer of content, this does not mean the online provider "enjoy[s] absolute immunity from all claims related to their content-neutral tools."[120] Because the suit focused on the negligent design of the neutral tool, Snap was still susceptible to liability and not granted immunity under Section 230.[121]

---

109. *Id.* at 1172.

110. *Id.* at 1174–75.

111. *Id.* at 1174.

112. *Id.* at 1175.

113. *Id.*

114. *See, e.g.*, Jones v. Dirty World Ent. Recordings, LLC, 755 F.3d 398, 413 (6th Cir. 2014); Henderson v. Source for Pub. Data, L.P., 53 F.4th 110, 127–28 (4th Cir. 2022); Force v. Facebook, Inc., 934 F.3d 53, 68–70 (2d Cir. 2019).

115. 570 F.3d 1187, 1199–200 (10th Cir. 2009).

116. *Id.* at 1201.

117. *Id.*

118. Lemmon v. Snap, Inc., 995 F.3d 1085, 1094 (9th Cir. 2021).

119. *Id.* at 1087.

120. *Id.* at 1094.

121. *Id.* at 1092.

The First Circuit case, *Doe v. Backpage.com, LLC*, is an outlier to the material contribution and neutral tools analysis.[122] There, the First Circuit held that Section 230 protected Backpage from liability for posts on the website that facilitated sex trafficking.[123] Backpage functioned as an online classified advertising site and enabled users to post and view advertisements that included "Adult Entertainment" and the subcategory, "Escorts."[124] Additionally, the online provider "tailored its posting requirements to make sex trafficking easier."[125] Even though Backpage materially contributed to the development of the illegal content and provided users with non-neutral tools, the court believed that Section 230 prohibited Backpage from being treated as an information content provider.[126] Former Congressman Christopher Cox, one of the coauthors of Section 230, explained that "[the First Circuit's] holding completely ignored the definition subsection (f)(3) of Section 230, which provides that anyone—including a website—can be an 'information content provider' if they are 'responsible, in whole or in part, for the creation or development' of online content."[127] In fact, Congressman Cox emphasized that "[i]t is difficult to imagine a clearer case of complicity 'in part, for the creation or development' of illegal content."[128]

4. Section 230 and Preemption of State Law

Section 230(e)(3) explicitly prohibits states from passing legislation imposing liability upon online service providers that is "inconsistent" with Section 230.[129] State legislation can be preempted by Section 230 in two ways: express and implied preemption.[130] A state law is expressly preempted by Section 230(c)(1) when the law treats an online service provider as the publisher of another user's content.[131] A state law can also be expressly preempted by Section 230 where it conflicts with Section 230(c)(2) and requires online providers to remove third-party content.[132] To determine whether a state law is impliedly preempted by Section 230, courts consider if the state law imposes an "obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[133]

---

122. *See* 817 F.3d 12, 22–24 (1st Cir. 2016).

123. *Id.* at 22 ("We hold that claims that a website facilitates illegal conduct through its posting rules necessarily treat the website as a publisher or speaker of content provided by third parties and, thus, are precluded by [S]ection 230(c)(1).").

124. *Id.* at 16.

125. *Id.*

126. *See id.* at 22.

127. *The PACT Act and Section 230: The Impact of the Law That Helped Create the Internet and an Examination of Proposed Reforms for Today's Online World: Hearing Before the S. Comm. on Com., Sci., & Transp.*, 116th Cong. 11 (2020) (statement of Christopher Cox, Couns., Morgan, Lewis & Bockius, LLP).

128. *Id.*

129. 47 U.S.C. § 230(e)(3).

130. Gade v. Nat'l Solid Wastes Mgmt. Ass'n, 505 U.S. 88, 98 (1992).

131. Backpage.com, LLC v. McKenna, 881 F. Supp. 2d 1262, 1273 (W.D. Wash. 2012).

132. *See* HomeAway.com, Inc. v. City of Santa Monica, 918 F.3d 676, 683 (9th Cir. 2019) (holding that an ordinance was not expressly preempted by Section 230 since it did not "proscribe, mandate, or even discuss" the content the platform displayed on its website).

133. Crosby v. Nat'l Foreign Trade Council, 530 U.S. 363, 373 (2000) (quoting Hines v. Davidowitz, 312 U.S. 52, 67 (1941)).

The Supreme Court of Florida, in *Doe v. America Online, Inc.*, held in 2001 that even though a state claim for negligence was properly pleaded against an online provider, Section 230 preempted the claim.[134] In the case, a mother brought suit against AOL because a user was utilizing AOL's chat rooms to sell photographs and videotapes of himself engaging in sexual activity with her eleven-year-old son and two other children.[135] The plaintiff argued that AOL was negligent in aiding in the sale and distribution of child pornography because AOL provided an avenue for the user to sell the material.[136] Additionally, the plaintiff claimed that even though AOL had been notified that the user was using the online platform to distribute obscene material, AOL took no action to stop the user.[137]

Using the analysis in *Zeran* and the legislative intent of Section 230 to support its reasoning, the Florida Supreme Court concluded that Section 230 preempted the state negligence claim against AOL.[138] Congress enacted Section 230 to address the decision in *Prodigy* and prevent liability for online providers for exercising editorial functions.[139] In *Doe*, the court explained that the state law negligence claim against AOL for failing to control content on its website expressly treated the online provider as a publisher and, therefore, was expressly in conflict with Section 230.[140]

B. Challenging Section 230's Broad Immunity

This Part explains the motivations behind California's new methods of liability.[141] Under California law, social media companies can be held liable for their failure to remove CSAM or for knowingly aiding in the commercial sexual exploitation of children.[142] California has not been the only entity to push back against Section 230. This Part also explores how many other lawmakers, including multiple sessions of Congress, state legislators, and a former U.S. attorney general, have urged reform or upheaval of Section 230 in order to address CSAM.[143]

1. California's Legislation Targeting Social Media Companies

California's Assembly Bill 1394 created two methods to hold social media platforms liable for contributing to online CSAM,[144] which went into effect on January 1, 2025.[145] The first method, embodied in Title 21 of the California Civil Code, "Child Sexual Abuse Material Hosted on a Social Media Platform" (CSAM-HSMP), provides

134. *See* 783 So. 2d 1010, 1013 (Fla. 2001).

135. *Id.* at 1011.

136. *Id.* at 1011–12.

137. *Id.*

138. *Id.* at 1013.

139. *Id.* at 1014–15 (quoting Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997)).

140. *See id.* at 1016–17 ("[A] publisher is not merely one who intentionally communicates defamatory information. Instead, the law also treats as a publisher or speaker one who fails to take reasonable steps to remove defamatory statements from property under her control." (quoting *Zeran*, 129 F.3d at 332)).

141. *See infra* Part II.B.1.

142. *See infra* Part II.B.1.

143. *See infra* Part II.B.2.

144. Assemb. B. 1394, 2023 Leg., Reg. Sess. (Cal. 2023).

145. *See* CAL. CIV. CODE §§ 3273.66–3273.69, 3345.1 (West 2025).

individuals with a private right of action to sue online providers for their failure to remove CSAM.[146] This statute requires social media platforms to create a CSAM reporting system for users residing in California.[147] Failure to create this reporting mechanism, to remove reported CSAM within specified time frames, or to make reasonable efforts to prevent other related material from being viewed are all potential ways a social media platform could be held liable by the reporting user for statutory damages.[148] The second avenue for liability, under section 3345.1 of the California Civil Code, arises where a social media platform "knowingly facilitate[s], aid[s], or abet[s] [the] commercial sexual exploitation" of minors.[149]

Before explaining the new requirements for social media platforms, the California State Legislature provided a list of findings that motivated them to enact this law.[150] It explained that social media platforms are often used to "facilitate the sexual abuse, exploitation, and trafficking of children."[151] Even though social media platforms are "aware of this issue," the legislature noted that they have not acted to address the problem.[152] The legislature also noted two instances of social media platforms failing to address CSAM: one involving Facebook and another involving TikTok.[153]

The legislature highlighted that a Facebook whistleblower provided a sworn statement to the U.S. Securities and Exchange Commission (SEC) explaining the social media platform's failure to address CSAM.[154] The statement asserted that Facebook's efforts to prevent the sexual abuse of children were "inadequate" and "underresourced."[155] More specifically, the whistleblower explained that Facebook does not track the full scale of CSAM on its platforms and "executives refuse to spend funds available."[156] Nor are Facebook's moderators "sufficiently trained."[157] In fact, Facebook is actually "ill-prepared to prevent child sexual abuse."[158] Finally, based on the statement to the SEC, the legislature emphasized that Facebook Groups are used to "facilitat[e] harm and child sexual abuse."[159] Specifically, it noted that the design of Facebook's Groups feature "allows sexual predators to use code words to describe the type of child" and "type of sexual activity."[160] Sexual predators also utilize Facebook's encrypted messaging to share these code words.[161]

146. *Id.* §§ 3273.66–3273.67.
147. *Id.* § 3273.66.
148. *See id.* §§ 3273.66–3273.67.
149. *Id.* § 3345.1(g)(1).
150. Assemb. B. 1394, 2023 Leg., Reg. Sess. (Cal. 2023).
151. *Id.* § 1(a).
152. *Id.*
153. *Id.* § 1(b)–(c).
154. *Id.* § 1(b).
155. *Id.* § 1(b)(1).
156. *Id.* § 1(b)(2).
157. *Id.* § 1(b)(3).
158. *Id.*
159. *Id.* § 1(b)(4).
160. *Id.*
161. *Id.*

The California State Legislature noted that a recent review of TikTok livestreams by Forbes Magazine found that viewers use the comment section to encourage and pay for acts of child pornography.[162] Viewers of the livestream will request young users to perform acts and then reward them for their performance with payments to Venmo, PayPal, or Cash App, or by sending the user TikTok gifts that can be redeemed for money.[163] The legislature finished by highlighting that an associate at Harvard's Berkman Klein Center for Internet & Society explained that this is "the digital equivalent of going down the street to a strip club filled with [fifteen]-year-olds."[164]

With these findings in mind, California's CSAM-HSMP adopts preestablished terms under federal law to explain the new framework social media platforms are required to follow.[165] First, "child pornography" is defined by Section 2256 of Title 18 of the U.S. Code[166]:

> [A]ny visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where—
>
> > (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
> >
> > (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
> >
> > (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.[167]

CSAM-HSMP also adopts the definition of "identifiable minor" from Section 2256,[168] which defines the term as a person who is "recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic" and either "was a minor at the time the visual depiction was created, adapted, or modified" or "whose image as a minor was used in creating, adapting, or modifying the visual depiction."[169] Under the law, CSAM is defined as child pornography or "[o]bscene matter that depicts a minor personally engaging in, or personally simulating, sexual conduct."[170]

CSAM-HSMP also defines a social media company and social media platform.[171] Both terms borrow their definitions from section 22675 of the California Business and Professions Code.[172] A "social media company" is defined as a "person or entity that

---

162. *Id.* § 1(c).
163. *Id.*
164. *Id.*
165. CAL. CIV. CODE § 3273.65 (West 2025).
166. *Id.* § 3273.65(a).
167. 18 U.S.C. § 2256(8).
168. CIV. § 3273.65(c).
169. 18 U.S.C. § 2256(9).
170. CIV. § 3273.65(b).
171. *Id.* § 3273.65(g)–(h).
172. *Id.* § 3273.65(g)(1), (h)(1).

owns or operates one or more social media platforms."[173] A "social media platform" is defined as an internet-based service that has users in California and meets two requirements: (1) a substantial function of the platform is to connect users and allow them to interact, and (2) the platform allows users to create public profiles and create or post content for other users.[174]

CSAM-HSMP presents social media platforms with the possibility of liability by requiring them to create a reporting mechanism to address CSAM.[175] The reporting mechanism must provide a "reasonably accessible" method for California residents to report material that meets three criteria: "(1) The reported material is [CSAM]. (2) The reporting user is an identifiable minor depicted in the material. (3) The reported material is displayed, stored, or hosted on the social media platform."[176] The material must be blocked by the social media platform if there is a "reasonable basis" to believe that it is CSAM, the material is actually present on the platform, and the report contains information on where to locate the material.[177] In addition to removing the reported CSAM, CSAM-HSMP requires social media platforms to "make reasonable efforts to remove and block other instances of the same reported material."[178]

The social media platform is then required to contact the reporting user and update them throughout the process at specified times.[179] Within thirty days of the initial report, the social media platform must inform the user about the final determination.[180] The social media platform has three options for the final determination report.[181] First, it can inform the reporting user that the material was determined to be CSAM that was displayed, stored, or hosted on the platform and that it has been blocked.[182] Second, it can tell the reporting user that the material was not found to be CSAM.[183] Or third, the social media platform can report that the CSAM was found to not be displayed, stored, or hosted on the platform itself.[184]

Any social media company that fails to meet these above requirements can be held liable to the reporting user for actual damages, fees, statutory damages, and "[a]ny other relief that the court deems proper."[185] The actual damages in a claim must arise due to the social media platform's failure to comply with the statute.[186] Additionally, the legislature built in a rebuttable presumption that the reporting user is entitled to statutory

173. CAL. BUS. & PROF. CODE § 22675(e) (West 2025).

174. *Id.* § 22675(f).

175. *See* CIV. § 3273.66(a).

176. *Id.*

177. *Id.* § 3273.66(d)(1).

178. *Id.* § 3273.66(d)(2).

179. *See id.* § 3273.66(c), (e) (requiring social media platforms to inform reporting users that the report was received within thirty-six hours of the report and requiring social media platforms to contact reporting users within seven days of the report to inform them of how they are handling the content).

180. *Id.* § 3273.66(h)(1).

181. *Id.* § 3273.66(g).

182. *Id.* § 3273.66(g)(1).

183. *Id.* § 3273.66(g)(2).

184. *Id.* § 3273.66(g)(3).

185. *Id.* § 3273.67(a).

186. *Id.* § 3273.67(a)(1).

damages where the social media platform fails to meet the requirements of the statute within sixty days of the report.[187] Statutory damages are limited to $250,000 per violation.[188] They can be further limited to $125,000 per violation if the social media platform blocks the reported material before a complaint is filed.[189] If the social media platform takes multiple steps in addressing the CSAM and works extensively with the NCMEC, statutory damages are again reduced to $75,000 per violation.[190] In determining statutory damages, courts are permitted to consider whether a social media platform has previously violated the statute and the "willfulness and severity of the violation."[191]

In addition to violations of the above requirements, under section 3345.1, social media platforms can also be held liable to victims of sexual exploitation for "knowingly facilitat[ing], aid[ing], or abet[ting] commercial sexual exploitation."[192] Under this new law, "commercial sexual exploitation" is defined as any act "committed for the purpose of obtaining property, money, or anything else of value in exchange for, or as a result of, a sexual act of a minor."[193] Platforms that violate this provision are subject to statutory damages ranging from one to four million dollars for "each act of commercial sexual exploitation facilitated, aided, or abetted."[194] A social media platform acts knowingly if the material at issue is displayed on the platform after January 1, 2025, is reported for four consecutive months, and meets the same three requirements for reporting as CSAM-HSMP.[195] Social media platforms "facilitate, aid, or abet" when they "deploy a system, design, feature, or affordance that is a substantial factor in causing minor users to be victims of commercial sexual exploitation."[196]

Social media companies can escape liability for "knowingly facilitat[ing], aid[ing], or abet[ting] commercial sexual exploitation" by meeting listed requirements.[197] First, the company must implement a program to biannually check features that can lead to sexual exploitation.[198] Second, within thirty days of each audit, the platform must take action to mitigate the risk of harm.[199] Finally, the board of directors must be provided with a copy of the audit and the action taken within ninety days of each audit.[200]

187. *Id.* § 3273.67(b).

188. *Id.* § 3273.67(a)(2)(A)(i).

189. *Id.* § 3273.67(a)(2)(A)(ii).

190. *Id.* § 3273.67(a)(2)(A)(iii).

191. *Id.* § 3273.67(a)(2)(B).

192. *Id.* § 3345.1(a), (g).

193. *Id.* § 3345.1(h)(1).

194. *Id.* § 3345.1(g)(2).

195. *Id.* § 3345.1(g)(4); *see id.* § 3273.66(a) ("(1) The reported material is child sexual abuse material. (2) The reporting user is an identifiable minor depicted in the reported material. (3) The reported material is displayed, stored, or hosted on the social media platform.").

196. *Id.* § 3345.1(g)(5).

197. *Id.* § 3345.1(g).

198. *Id.* § 3345.1(g)(3)(A).

199. *Id.* § 3345.1(g)(3)(B).

200. *Id.* § 3345.1(g)(3)(C).

2. Reform Proposals for Section 230

While California has passed a law directly addressing the proliferation of online CSAM, other actors have chosen to call for Section 230 reform as the first step. Many legislators have proposed amendments to Section 230 because of the expansive immunity granted to online providers.[201] Since 2019, the 116th, 117th, and 118th Congresses have each proposed more than a dozen bills to amend Section 230.[202] The proposals range from repealing Section 230 entirely[203] to limiting the expansive scope of its immunity.[204] Proposals to limit the statute's immunity focus on amending Section 230(e) and providing additional exceptions to liability immunity.[205] For example, the Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment (STOP CSAM) Act of 2023 focuses on creating an additional carve out for liability for interactive computer services that post CSAM and fail to remove the content after being notified of its existence.[206] Additionally, state legislators have called on Congress to amend Section 230.[207] One of these proposals came from the New Jersey legislature, which was concerned with Section 230's potential to preempt New Jersey state law targeting child sexual exploitation material.[208]

In 2020, then-U.S. Attorney General William P. Barr called on Congress to amend Section 230.[209] Notably, Attorney General Barr proposed updating Section 230 to account for the "drastic" changes the internet has undergone since 1996.[210] Online platforms are "no longer nascent companies but have become titans of industry."[211] He also highlighted that courts interpreted Section 230 broadly and expanded immunity far beyond what was initially intended.[212] Some platforms have used Section 230 immunity to elude "liability even when they knew their services were being used for criminal activity."[213]

---

201. VALERIE C. BRANNON & ERIC N. HOLMES, CONG. RSCH. SERV., R46751, SECTION 230: AN OVERVIEW 32–39 (2024).

202. *Id.* at 32; *Section 230 Legislation Tracker*, LAWFARE, https://www.lawfaremedia.org/projects-series/lawfare-research-intiative/section-230-tracker [https://perma.cc/YB3L-5T7J] (last visited Oct. 20, 2025).

203. *E.g.*, A Bill To Repeal Section 230 of the Communications Act of 1934, S. 2972, 117th Cong. § 1 (2021).

204. *E.g.*, A Bill To Waive Immunity under Section 230 of the Communications Act of 1934 for Claims and Charges Related to Generative Artificial Intelligence, S. 1993, 118th Cong. § 1 (2023) (proposing an amendment to waive immunity provided by Section 230 for claims concerning generative artificial intelligence).

205. *See* BRANNON & HOLMES, *supra* note 201, at 32–34.

206. S. 1199, 118th Cong. § 2260B (2023) (amending Section 230 to allow interactive computer service providers to be held liable for claims involving CSAM).

207. *E.g.*, H. Mem'l 23, 2022 Leg., Reg. Sess. (Fla. 2022) (urging Congress to repeal Section 230).

208. *See* Assemb. Con. Res. 117, 220th Leg., Reg. Sess. (N.J. 2022) (requesting Congress to amend Section 230 to prevent preemption of state laws aimed at addressing child sexual exploitation).

209. Letter from William P. Barr, U.S. Att'y Gen., to Michael R. Pence, President of the U.S. S. 1 (Sep. 23, 2020), https://www.justice.gov/ag/media/1093246/dl?inline= [https://perma.cc/FCX8-YJLZ].

210. *Id.*

211. *Id.*

212. *Id.* at 2.

213. *Id.*

The proposal called for three main amendments.[214] First, it recommended updates to vague terms within Section 230 to protect users' free speech rights.[215] Second, the amendments would add additional exclusions from liability, specifically when online providers purposefully promote content that violates federal law or fail to remove unlawful content.[216] Granting immunity to online providers from liability for hosting illicit content, Attorney General Barr claimed, is in fact "inconsistent with the purpose of Section 230 . . . to encourage platforms to make the internet a safer place for children."[217] Consistent with the stated purpose of Section 230, he called for three specific exceptions from immunity: "(1) child exploitation and sexual abuse; (2) terrorism; and (3) cyber-stalking."[218] Finally, the proposal suggested that the federal government should be permitted to pursue civil claims against online providers.[219]

Attorney General Barr's proposal shows the weight and urgency of reforming Section 230. This proposal was released by the Department of Justice in 2020 after a ten-month review.[220] The review included conversations with the public, experts, industry members, and policymakers to understand the problems with Section 230.[221] While there have been numerous calls to amend Section 230, since the enactment of FOSTA in 2018, no proposal has been passed.[222]

C. Online Content and the First Amendment

Content on online platforms implicates not only Section 230, but also the broad speech protections afforded by the First Amendment.[223] The First Amendment provides protection for users and online providers.[224] Where an online provider creates an "expressive product," it will receive the protection of the First Amendment.[225] Online providers create constitutionally protected "expressive" content when they make decisions about what third-party speech to display and how to display it.[226] This is the

214. *Id.* at 2–4.

215. *Id.* at 2–3.

216. *Id.* at 3–4.

217. *Id.* at 3.

218. *Id.* at 4.

219. *Id.*

220. *Justice Department Issues Recommendations for Section 230 Reform*, U.S. DEP'T OF JUST. (June 17, 2020), https://www.justice.gov/archives/opa/pr/justice-department-issues-recommendations-section-230-reform [https://perma.cc/9EJ9-CV29].

221. *Id.*

222. *See* 47 U.S.C. § 230; BRANNON & HOLMES, *supra* note 201, at 2, 26–32.

223. *See* Packingham v. North Carolina, 137 S. Ct. 1730, 1732 (2017) ("Today, one of the most important places to exchange views is cyberspace, particularly social media, which offers 'relatively unlimited, low-cost capacity for communication of all kinds,' to users engaged in a wide array of protected First Amendment activity on any number of diverse topics." (quoting Reno v. ACLU, 521 U.S. 844, 870 (1997))).

224. *See* 303 Creative LLC v. Elenis, 143 S. Ct. 2298, 2312 (2023) (holding that a website that contains third-party content is still protected under the First Amendment for the "pure speech" contained in the website's design).

225. Moody v. NetChoice, LLC, 144 S. Ct. 2383, 2393 (2024).

226. *Id.*

same speech protection that traditional editors and publishers hold when editing material for publication.[227]

In *Moody v. NetChoice, LLC*, the U.S. Supreme Court explained how to determine if a statute violates the First Amendment on its face.[228] The Court considered two state laws, one from Florida and another from Texas, that the Fifth and Eleventh Circuits, respectively, analyzed.[229] The Florida statute limited social media platforms' ability to delete posts based on their content and required the platforms to provide explanations to users who had their post altered or removed.[230] Like the Florida statute, the Texas law prohibited social media platforms from blocking users' content and required the platform to explain why content was removed.[231] The Fifth and Eleventh Circuits disagreed on whether these laws, on their face, triggered First Amendment scrutiny.[232]

The Supreme Court explained that the first step in analyzing whether a state law is facially unconstitutional is to consider the law's scope.[233] This includes considering the activities and actors the law regulates and how the law affects other services on the platform, such as direct messaging.[234] The second step is to determine if any applications of the law violate the First Amendment.[235] A law violates the First Amendment for content moderation where "there is an intrusion on protected editorial discretion."[236] Because the lower courts had not conducted a factual inquiry based on these requirements, the Supreme Court remanded these cases.[237]

The Supreme Court took a moment to correct the Fifth and Eleventh Circuit Courts' misunderstanding of the First Amendment's protection for online providers.[238] Importantly, forcing a publisher to print material violates the First Amendment because it interferes with the "exercise of editorial control and judgment."[239] Editorial control is a part of speech that is protected by the First Amendment.[240] This is true when an online provider is publishing or editing content from third parties and when it is creating its own content.[241] Even though these principles of speech protection emerged under the more brick-and-mortar counterparts to online publishers, the Supreme Court emphasized that as technology advances "the basic principles of the First Amendment do not vary."[242]

---

227. *Id.*

228. *Id.* at 2398–99.

229. *Id.* at 2395–97.

230. *Id.* at 2395.

231. *Id.* at 2396.

232. *Id.*

233. *Id.* at 2398.

234. *Id.*

235. *Id.*

236. *Id.*

237. *Id.* at 2399.

238. *Id.*

239. *Id.* at 2400 (quoting Mia. Herald Publ'g Co. v. Tornillo, 418 U.S. 241, 258 (1974)).

240. *Id.* at 2401–02 (quoting Denv. Area Educ. Telecomms. Consortium, Inc. v. FCC, 518 U.S. 727, 737 (1996)).

241. *Id.* at 2402.

242. *Id.* at 2403 (internal quotation marks omitted) (quoting Brown v. Ent. Merchs. Ass'n, 564 U.S. 786, 790 (2011)).

Laws that attempt to regulate online speech based on content are unconstitutional if they do not satisfy strict scrutiny.[243] A law will be unconstitutional when it is overly broad and chills freedom of speech.[244] Where there are equally effective methods to achieve a law's legitimate purpose that do not unduly burden speech, the law is considered unconstitutionally broad.[245] For example, in *Reno v. ACLU*, the Supreme Court determined that an initial portion of the CDA, which prohibited the transmission of indecent or obscene messages to minors, was unconstitutionally broad under the First Amendment.[246] Because the prohibition used vague words, such as "indecent" and "patently offensive," to prohibit online speech, the Court determined that this portion of the CDA was not narrowly tailored and suppressed constitutionally protected speech.[247] While the government's interest in protecting children from harmful material is legitimate, the Court explained that this interest does not allow "an unnecessarily broad suppression of speech addressed to adults."[248]

The Supreme Court reaffirmed this position in *Ashcroft v. Free Speech Coalition*.[249] While the First Amendment protects freedom of speech, this freedom has limits.[250] The freedom does not extend to categories such as defamation, obscenity, and pornography created using real children.[251] Because the law in question in *Ashcroft*, the Child Pornography Prevention Act of 1995, attempted to criminalize virtual child pornography created through computer-imaging technology, the Court determined that the material was neither obscene nor pornography created using real children.[252] Because virtual child pornography did not fit into either of these exceptions, the Court emphasized that the speech was protected under the First Amendment.[253] The Court then reiterated that the government cannot censor unprotected speech "if a substantial amount of protected speech is prohibited or chilled in the process."[254]

III. DISCUSSION

This Section argues that California's CSAM-HSMP would likely be preempted by Section 230's current immunity provisions for online providers. Part III.A contends that CSAM-HSMP and section 3345.1 are not unconstitutional under the First Amendment; however, CSAM-HSMP is preempted by Section 230. Part III.B argues that section 3345.1, which treats social media platforms as information content providers for the content they materially contributed to, is allowed under Section 230. Part III.C

243. *See* Reno v. ACLU, 521 U.S. 844, 874 (1997) (holding that "content-based" regulation of speech suppresses a constitutionally protected right).

244. NetChoice, LLC v. Paxton, 49 F.4th 439, 450 (5th Cir. 2022).

245. *Reno*, 521 U.S. at 874.

246. *Id.*

247. *Id.* at 874 ("Sexual expression which is indecent but not obscene is protected by the First Amendment." (quoting Sable Commc'ns of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989))).

248. *Id.* at 875.

249. 535 U.S. 234, 245 (2002).

250. *Id.*

251. *Id.* at 245–46.

252. *Id.* at 239–40, 250–51.

253. *Id.* at 256.

254. *Id.* at 255.

recommends Congress revisit Section 230's broad immunity and introduce amendments to allow laws, like California's, to effectively address online CSAM.

A. California's New Law Is Facially Constitutional, but CSAM-HSMP Is Preempted by Section 230

Because content published online implicates issues of freedom of speech,[255] before addressing the constitutionality of California's new law with respect to Section 230 preemption, it must be facially constitutional under the First Amendment. A facial challenge would likely not be successful as the scope of California's law is narrowly tailored to achieve a legitimate goal.[256] However, the reporting mechanism and subsequent liability for failure to conform with these requirements that CSAM-HSMP enforces on social media platforms[257] is expressly preempted by Section 230 since it requires online providers to remove third-party content.[258] This method of liability is also impliedly preempted as it poses an obstacle to the dual purposes of Section 230.[259] However, the second avenue for liability under section 3345.1, which allows a social media platform to be sued for "knowingly facilitat[ing], aid[ing], or abet[ting] commercial sexual exploitation,"[260] is not preempted as it is consistent with Section 230 liability.[261]

1. The First Amendment Does Not Preclude California from Regulating Online Content Through CSAM-HSMP

While social media platforms facing liability under CSAM-HSMP may attempt a facial challenge based on the First Amendment, this claim would likely be unsuccessful. The First Amendment does provide protection to social media platforms for editorial decisions they make on what content they display.[262] However, a facial challenge based on freedom of speech requires considering the scope of the law to determine if the law is unconstitutionally broad.[263] Whereas the laws in *Moody* required social media platforms to moderate content on *every single* post by *every single* user,[264] CSAM-HSMP

255. *See* Packingham v. North Carolina, 137 S. Ct. 1730, 1732 (2017) ("Today, one of the most important places to exchange views is cyberspace, particularly social media, which offers 'relatively unlimited, low-cost capacity for communication of all kinds,' to users engaged in a wide array of protected First Amendment activity on any number of diverse topics." (quoting Reno v. ACLU, 521 U.S. 844, 870 (1997))).

256. *See* Moody v. NetChoice, LLC, 144 S. Ct. 2383, 2394 (2024).

257. CAL. CIV. CODE §§ 3273.66–3273.67 (West 2025).

258. *See* HomeAway.com, Inc. v. City of Santa Monica, 918 F.3d 676, 683 (9th Cir. 2019).

259. *See* Doe v. Am. Online, Inc., 783 So. 2d 1010, 1016 (Fla. 2001) (quoting Zeran v. Am. Online, Inc., 958 F. Supp. 1124, 1132–35 (E.D. Va. 1997)); *see also* 141 CONG. REC. 22045 (1995) (statement of Rep. Christopher Cox) (explaining the dual purposes of Section 230 as (1) protecting Good Samaritans and online service providers from liability for screening offensive material and (2) establishing as policy that the United States does not want the government regulating internet content).

260. CIV. § 3345.1(g)(1).

261. *See* 47 U.S.C. § 230(e)(3).

262. *See* Moody v. NetChoice, LLC, 144 S. Ct. 2383, 2393 (2024).

263. Reno v. ACLU, 521 U.S. 844, 874 (1997).

264. *See Moody*, 144 S. Ct. at 2395–96.

only requires social media platforms to regulate very specific content.[265] First, the content must have been reported by a California user of the social media platform.[266] Then, the platform only needs to consider whether to remove content that is reported by California users who believe the content is CSAM depicting the reporter.[267] The scope of this law is much narrower than the laws considered in *Moody*.

Reno also serves as an important point of comparison for CSAM-HSMP. While in *Reno* the Supreme Court determined the challenged portion of the CDA was unconstitutionally broad due to prohibitions on vague terms such as "indecent" and "patently offensive" online speech,[268] no such language can be found in California's law. For one, the California legislature took care to define each term utilized in CSAM-HSMP.[269] Additionally, as recognized in *Reno*, a government's interest in protecting children from harmful material is a legitimate state interest.[270] This is aligned with CSAM-HSMP's goal of addressing the sexual abuse, exploitation, and trafficking of children that occurs on social media platforms.[271]

Finally, the material covered by CSAM-HSMP is not speech protected under the First Amendment.[272] As the Supreme Court recognized in *Ashcroft*, pornography that is created using real children is not a category that is protected under the First Amendment.[273] CSAM-HSMP by its definition only concerns pornography involving "real children."[274] A person reporting the child pornography hosted on a social media platform must be the identifiable minor in the content.[275] This requirement prevents social media platforms from arguing that CSAM-HSMP censors speech protected by the First Amendment as the Court determined in *Ashcroft*.[276]

2. CSAM-HSMP Is Expressly Preempted by Section 230 Because the Statute Imposes Liability Inconsistent with Section 230

The first avenue of liability for social media platforms under CSAM-HSMP is expressly preempted by Section 230 as it requires online providers to remove third-party content.[277] Section 230(e)(3) directly explains that states cannot pass legislation that

265. *See* CIV. § 3273.66(a)(1)–(3).

266. *Id.* § 3273.66(a).

267. *Id.* § 3273.66(d)(1)(A)–(C)(ii).

268. *Reno*, 521 U.S. at 874–75, 878.

269. *See* CIV. § 3273.65 (defining terms such as "social media platform," "child pornography," and "child sexual abuse material").

270. *Reno*, 521 U.S. at 875.

271. Assemb. B. 1394, 2023 Leg., Reg. Sess. (Cal. 2023).

272. *See* Ashcroft v. Free Speech Coal., 535 U.S. 234, 245–46 (2002) (explaining that freedom of speech has limits).

273. *Id.*

274. *See* CIV. § 3273.65(c) (adopting the definition of "identifiable minor" from 18 U.S.C. § 2256(9)).

275. *Id.* § 3273.66(a)(2).

276. *See Ashcroft*, 535 U.S. at 251, 255 (holding that virtual child pornography created by computers is protected speech under the First Amendment since the pornography was not created using real children).

277. *See* CIV. § 3273.66(d)(1); *see also* HomeAway.com, Inc. v. City of Santa Monica, 918 F.3d 676, 683 (9th Cir. 2019) (holding an ordinance was not expressly preempted by Section 230 since it did not "proscribe, mandate, or even discuss" the content the platform displayed on its website).

imposes liability inconsistent with the federal law.[278] This first path of liability under CSAM-HSMP is inconsistent with Section 230(c)(2), which immunizes online providers from liability for their choice to remove obscene, violent, or objectionable material hosted on their site.[279] The second option for liability under section 3345.1—for knowingly facilitating, aiding, or abetting commercial sexual exploitation—is consistent with Section 230 since it treats the social media platforms as information content providers for their contributions to the content.[280]

Zeran serves as an important case comparison. By its application, CSAM-HSMP requires social media platforms to remove material hosted on the site that meets three criteria: the material is CSAM, the reporting user is in the CSAM, and the material is on the social media platform.[281] If a social media platform fails to remove the CSAM, it faces the possibility of being held liable for damages to the reporting user.[282] As in *Zeran* where the plaintiff claimed that the online provider could be held liable for its failure to remove defamatory material after being given notice of its existence, CSAM-HSMP requires social media platforms to remove content after being given notice.[283] However, as discussed in *Zeran*, under Section 230, online providers are immune from liability for their role as the publisher of content created by a third party.[284] As the Fourth Circuit explained, when online providers are given notice of content that should be removed, they are "thrust into the role of a traditional publisher," a role that finds immunity under Section 230.[285] Just as the plaintiff's argument was dismissed in *Zeran*,[286] Section 230 would provide social media platforms with immunity from CSAM-HSMP in the same way.[287]

The second avenue of liability for social media platforms under section 3345.1 is not inconsistent with nor expressly preempted by Section 230. By the definitions outlined by the law, California would create liability for social media platforms for their role as independent information content providers.[288] Section 3345.1 does not treat the platforms as the "publisher or speaker of any information provided by another information content provider," as prohibited by Section 230.[289] Instead, it provides that social media platforms can be held liable for knowingly facilitating, aiding, or abetting the commercial sexual exploitation of minors.[290] It becomes clear from the definitions provided in section 3345.1 that liability under this provision seeks to hold social media

278. 47 U.S.C. § 230(e)(3).

279. *See id.* § 230(c)(1)–(2).

280. *See id.* § 230(c)(1); CIV. § 3345.1(g)(1).

281. CIV. § 3273.66(a)(1)–(3).

282. *Id.* § 3273.67(a).

283. Zeran v. Am. Online, Inc., 129 F.3d 327, 328 (4th Cir. 1997).

284. *Id.* at 332–33.

285. *Id.* at 332.

286. *Id.* at 333.

287. *See id.*

288. *See* CAL. CIV. CODE § 3345.1 (West 2025) (defining "facilitate, aid, or abet" as "deploy[ing] a system, design, feature, or affordance that is a substantial factor in causing minor users to be victims of commercial sexual exploitation").

289. *See* 47 U.S.C. § 230(c)(1).

290. CIV. § 3345.1(g)(1).

platforms accountable for their contributions to illicit content.[291] Under section 3345.1, by "deploy[ing] a system, design, feature, or affordance that is a substantial factor in causing minor users to be victims of commercial sexual exploitation,"[292] California seeks to hold social media platforms accountable for the role they had in creating the illicit content. This is consistent with Section 230 as online providers can be held liable for content that they were responsible in whole or in part for creating.[293]

3. CSAM-HSMP Is Inconsistent with the Dual Purposes of Section 230

CSAM-HSMP is impliedly preempted by Section 230 as it imposes an "obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[294] California's law is unique since it punishes social media platforms for the content they *fail* to remove rather than the content they publish, which directly conflicts with the dual purposes of Section 230.[295] Section 230 was enacted to avoid the outcome in *Prodigy* in which an online provider was held liable for failing to screen content hosted on the website.[296] By holding social media platforms liable for failing to screen content, CSAM-HSMP directly impedes the protection Section 230 was designed to provide for online providers.[297]

While proponents of Section 230 were interested in shielding minors from offensive and pornographic material,[298] courts do not consider this as one of the dual purposes of Section 230.[299] When analyzing whether immunity preempts state liability, courts have recognized that state laws are impliedly preempted where they obstruct Section 230's goals of minimizing government regulation of online content and encouraging online providers to self-regulate content.[300] CSAM-HSMP directly obstructs the second purpose of Section 230 by allowing content-reporting users and the California government to enforce content regulation on social media platforms rather than allowing the platforms to maintain the content themselves.[301]

---

291. See *infra* Part III.B for a discussion on holding online providers liable for their material contribution to illicit content.

292. CIV. § 3345.1(g)(5).

293. *See* 47 U.S.C. § 230(f)(3); Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1162–63 (9th Cir. 2008).

294. *See* Crosby v. Nat'l Foreign Trade Council, 530 U.S. 363, 373 (2000) (quoting Hines v. Davidowitz, 312 U.S. 52, 67 (1941)).

295. *See* 141 CONG. REC. 22045 (1995) (statement of Rep. Christopher Cox) (explaining the dual purposes of Section 230 as (1) protecting Good Samaritans and online service providers from liability for screening offensive material and (2) establishing as policy that the United States does not want the government regulating internet content); *see also* Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997) (holding that imposing liability on an online provider after it failed to remove content that a user reported "defeat[s] the dual purposes" of Section 230).

296. *See* 141 CONG. REC. 22045 (1995) (statement of Rep. Christopher Cox).

297. *See id.*

298. *Id.*

299. *See Zeran*, 129 F.3d at 330 ("Section 230 was enacted . . . [(1)] to maintain the robust nature of Internet communication and . . . [(2)] to keep government interference in the medium to a minimum.").

300. *Id.* at 330–31.

301. *See* CAL. CIV. CODE § 3273.66 (West 2025).

On the other hand, the second method of liability under section 3345.1 is not impliedly preempted by Section 230. As explained by the most recent amendment to Section 230, FOSTA, immunity for online providers was "never intended to provide legal protection to websites that unlawfully promote and facilitate prostitution and websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims."[302] Section 3345.1 intends to hold online providers accountable for their role in facilitating and aiding commercial sexual exploitation of minors, directly in compliance with Section 230.[303]

B. California Can Regulate Online Content by Treating Social Media Platforms as Developers for Their Material Contribution to Illicit Content

The second method of liability under section 3345.1 holds social media platforms accountable for the material contributions they make to content.[304] An online provider can be liable under Section 230 for their role as an information content provider.[305] Online providers, like social media platforms, become information content providers where they materially contribute to the development of the content in whole or in part.[306] Section 3345.1 recognizes that social media platforms are not simply providing neutral tools that users utilize for CSAM, which maintains Section 230 immunity, but instead attempts to hold platforms liable where they materially contribute to the development of CSAM.[307]

Section 3345.1 focused on holding social media platforms liable for their own collaboration on online content, specifically for creating features or designs that are a "substantial factor in causing minor users to be victims of commercial sexual exploitation."[308] *Roommates.com* serves as an essential case comparison. The Ninth Circuit explained that the online provider in the case functioned as an information content provider through its collaboration with users' illicit content.[309] In *Roommates.com*, the online provider had created options for users that contributed to illegal content.[310] The findings from California's legislature indicate that section 3345.1 is aimed at addressing social media platforms that have contributed to illegal content by creating systems that facilitate harm to children and are a substantial factor of that harm.[311]

If a court determined section 3345.1 to attribute liability to social media platforms for their neutral tools, this would still be allowed under Section 230. While providing

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

303. *See* CIV. § 3345.1.

304. *See id.* § 3345.1(g)(5) (defining "facilitate, aid, or abet" as "deploy[ing] a system, design, feature, or affordance that is a substantial factor in causing minor users to be victims of commercial sexual exploitation").

305. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1166 (9th Cir. 2008).

306. *See id.* at 1168.

307. *See* CIV. § 3345.1(g)(5).

308. *Id.*

309. *Roommates.com*, 521 F.3d at 1166.

310. *Id.*

311. Assemb. B. 1394, 2023 Leg., Reg. Sess. § 1 (Cal. 2023) (explaining two social media case studies—Facebook and TikTok—that have facilitated harm and child sexual abuse).

neutral tools to users, which are then used to create illicit content, does not amount to development under Section 230,[312] online providers can still be held liable for the design of their neutral tools.[313] In fact, just as in the Ninth Circuit case, *Lemmon*, a social media platform can still be held liable for its neutral tools, including features or designs, that are negligently designed.[314]

C. Congress Should Amend Section 230 To Allow Laws like California's To Fully Address Illicit Online Content

Because the first method for liability under California's Civil Code is preempted by Section 230[315] and there have been growing calls to reform Section 230,[316] Congress should revisit Section 230 and amend the scope of online providers' immunity. While legislatures and courts worry about the "impossible burden" of requiring online providers to moderate the vast content posted online,[317] new developments in technology require Section 230 to be revisited to ensure that obscene content, such as CSAM, does not continue to remain unchecked.[318] It is worrisome that, despite their knowledge, social media platforms have taken little to no action to address the use of their sites to "facilitate the sexual abuse, exploitation, and trafficking of children."[319] Rather than being the "Good Samaritans" Section 230 expected them to be,[320] online providers have enjoyed broad Section 230 immunity[321] and have continued to offer inadequate and under-resourced efforts to address CSAM hosted online.[322]

To truly ensure the internet remains a space of cultural development and intellectual activity,[323] rather than a breeding ground for illicit content, Section 230 must be amended to recognize that current Section 230 immunity prevents states, like California, from passing laws that work to effectively address CSAM. It should not be forgotten that one of the motivating factors behind Section 230 was to ensure that material online would not be harmful to children.[324]

---

312. *Roommates.com*, 521 F.3d at 1169.

313. *See* Lemmon v. Snap, 995 F.3d 1085, 1094 (9th Cir. 2021) ("[W]hile providing content-neutral tools does not render an internet company a 'creator or developer' of the downstream content that its users produce with those tools, our case law has never suggested that internet companies enjoy absolute immunity from all claims related to their content-neutral tools.").

314. *See id.*

315. See *supra* Part III.A for a discussion on how CSAM-HSMP is expressly and impliedly preempted by Section 230.

316. See *supra* Part II.B for a discussion on widespread proposals to amend or even repeal Section 230.

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

318. *See* Assemb. B. 1394, 2023 Leg., Reg. Sess. § 1 (Cal. 2023).

319. *See id.*

320. *See* 141 CONG. REC. 22045 (1995) (statement of Rep. Christopher Cox).

321. *See, e.g.*, Ricci v. Teamsters Union Loc. 456, 781 F.3d 25, 28 (2d Cir. 2015); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123–25 (9th Cir. 2003).

322. *See* Cal. Assemb. B. 1394 § 1(b)(1) (explaining that Facebook's efforts to prevent CSAM are "inadequate" and "underresourced").

323. *See* 47 U.S.C. § 230(b).

324. *See* 141 CONG. REC. 22044–45 (1995) (statement of Rep. Christopher Cox).

IV. CONCLUSION

In its current form, CSAM-HSMP is not an effective way to hold online providers liable for their contributions to the abuse of CSAM victims. Because CSAM-HSMP is preempted by Section 230, the full power of the legislation is limited. Even though there have been numerous calls to reform Section 230, since the adoption of FOSTA in 2018, there have been no new amendments. Instead of allowing legislation to address the growing issue of CSAM and the threat new technology poses in this arena, Section 230 continues to allow online providers to act as their own referees on the belief that they will be "Good Samaritans."[325]

Through its implementation by the legislature and later interpretation by the judiciary, the broad immunity granted to online providers leaves very few avenues for holding them accountable for the harm they perpetuate. When the proponents of Section 230 created the legislation, they were concerned with protecting children. Somewhere along the way, this goal was overshadowed by the desire to keep the government and regulatory oversight out of the internet. Now Section 230 can hardly claim to be concerned with protecting children when tens of millions of CSAM reports are made each year with no end in sight.

As this Comment has argued, Section 230 must be amended to address CSAM. Legislatures like California's must be allowed to act to protect one of the most vulnerable groups in the country: our children. No longer can social media companies and online providers be allowed to self-govern when many reports have shown they have put little to no effort into addressing the harm perpetuated on their sites. California's legislation offers a better path forward, one where online providers are forced to recommit to being the "Good Samaritans" online users need them to be.

325. *See* 47 U.S.C. § 230(c).