SECTION 230: THE VALYRIAN STEEL FOR WEBSITE OPERATORS, AND WHY A TAX CREDIT IS THE BEST SOLUTION TO A SAFER INTERNET

Noah Hale
SECTION 230: THE VALYRIAN STEEL FOR WEBSITE OPERATORS, AND WHY A TAX CREDIT IS THE BEST SOLUTION TO A SAFER INTERNET

Noah Hale*

TABLE OF CONTENTS

I. BACKGROUND .............................................................................................................. 282
II. CONGRESS’ INTENT IN ENACTING § 230 ................................................................. 283
III. HOW COURTS HAVE INTERPRETED § 230 ............................................................. 285
IV. SECTION 230(C)(2)’S GOAL TO ENCOURAGE CONTENT MONITORING, AND WHY IT FAILED ......................................................................................... 292
V. THE CRITICISM OFFERED TOWARDS § 230 .............................................................. 299
VI. THE SOLUTION: MAINTAIN § 230, BUT RESOLVE THIS INTERNET PROBLEM THROUGH TAX CREDITS ................................................................. 304
VII. WHY A TAX CREDIT IS A BETTER SOLUTION THAN A DIRECT SUBSIDY OR TAX DEDUCTION .................................................................................. 311
VIII. CONCLUSION ........................................................................................................... 314

Abstract

The most polarizing statute regulating the internet is § 230 of the Communications Decency Act. Critics of § 230 do not like that the statute provides broad immunity to website operators when third parties post on their sites, while advocates for § 230 market the statute as promoting free speech on the internet and preventing website operators from being subject to endless liability. Critics view the statute as the sole problem, and the advocates view § 230 as the savior for these website operators. But the problem of hate speech and hurtful content online is immense and requires expensive investment by these companies to mitigate misinformation and harmful content. We need to incentivize companies to invest in content moderation, tools, and

* My name is Noah Hale, and I am a law student at the Elisabeth Haub School of Law at Pace University. I am an Executive Productions Editor of PACE LAW REVIEW, and I want to thank PACE LAW REVIEW for giving me the opportunity to write this article and for all the help they have provided along the way. I am also grateful for my family, friends, and faculty who were supportive of me while writing this article.
personnel that will flag and remove dangerous content while being careful to not scare these companies with potentially endless liability and overwhelming costs. With so many tech companies struggling to achieve profitability, the solution lies in making content moderation less expensive in the short-term. Website operators should get a tax credit in the short-term to help bear the brunt of initial investments into content moderation. Once website operators have established artificial intelligence to flag and remove dangerous content, they will become less reliant on the tax credit, as they have established the essential assets needed to mitigate dangerous speech on their platforms. If companies are incentivized to invest in content moderation, rather than being scared with the potential of endless liability, we will be closer to achieving our goal of creating safer platforms for internet speech.

I. BACKGROUND

On April 25, 1995, an individual posted t-shirts on an online webpage that referred to the bombing of a federal building in Oklahoma City.1 The individual said in the online post that people interested in purchasing the t-shirts should call Ken Zeran, and included Zeran’s phone number.2 As a result of this prank, Zeran received a high number of derogatory messages and death threats.3

The same post was made again on April 26, 1995, and “interested buyers were told to call Zeran’s phone number . . . and ‘please call back if busy’ due to high demand.”4 By April 30, 1995, Zeran received a violent phone call approximately every two minutes.5 During this time period, Zeran notified America Online, Inc. (“AOL”), the owner of the website the post was written on, of the contents and extremities of the post. AOL did not take down the post.6

Can Zeran bring a successful lawsuit against AOL, the website operator, for defamatory speech of a third-party on

---

2. Id.
3. Id.
4. Id.
5. Id.
6. Id.
AOL’s webpage? No, Zeran cannot. The reason that Zeran and other victims of online defamatory statements cannot bring successful lawsuits against website operators is because of § 230 of the Communications Decency Act (“CDA”). “[Section] 230 creates a federal immunity” to claims that try to make website operators “liable for information originating with a third-party user of the service.”

II. CONGRESS’ INTENT IN ENACTING § 230

Congress enacted § 230 of the CDA on February 8, 1996. The statute states, “[n]o 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.” The term “interactive computer services” includes “anything from web hosts to websites to social media companies.” To analyze the statute by elements, § 230(c)(1) protects liability for “(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat . . . as a publisher or speaker (3) of information provided by another information content provider.”

Congress’ intentions for § 230 were, inter alia, to “promote the continued development of the Internet,” to preserve “the competitive free market that” exists for internet and computer services companies, and to “maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services.”

Congress also enacted § 230 in response to court cases that

7. See id.
8. See id. at 330–35.
11. Id. at 334; see 47 U.S.C. § 230.
13. Matt Laslo, The Fight Over Section 230—and the Internet as We Know It, WIRED (Aug. 13, 2019, 3:18 PM), https://www.wired.com/story/fight-over-section-230-internet-as-we-know-it/; see also Fair Hous. Council of San Fernando Valley v. Roomates.com, LLC, 521 F.3d 1157, 1162 n.6 (9th Cir. 2008) (“Today, the most common interactive computer services are websites.”).
held website operators liable for “defamatory statements” posted by third parties on website operators’ message boards.\textsuperscript{16} For example, in \textit{Stratton Oakmont v. Prodigy Services Company}, an unidentified user of Prodigy’s internet bulletin board titled “Money Talk” wrote a comment alleging that Stratton Oakmont and its President at the time committed “criminal and fraudulent acts in connection with the initial public offering of . . . Solomon-Page Ltd.”\textsuperscript{17} The New York Supreme Court determined that Prodigy controlled the content of its computer bulletin boards, as they had the technology to “delete notes from its computer bulletin boards on the basis of offensiveness and ‘bad taste.’”\textsuperscript{18} The court concluded that Prodigy was liable for defamation committed by its users.\textsuperscript{19}

According to Congress, § 230 has spurred significant advances for internet and computer services companies in “the availability of educational and informational resources to our citizens.”\textsuperscript{20} Internet users have “a great deal of control over the information they receive,” and people are relying on “interactive media for . . . political, educational, cultural, and entertainment services.”\textsuperscript{21} The internet and interactive computer services offer a forum of discussion for political, educational, cultural, and entertainment matters.\textsuperscript{22}

Section 230 has helped shape the internet into the influential and valuable product it now is. It has helped promote the free expression of different cultural views.\textsuperscript{23} The statute is

---


\textsuperscript{17} Stratton Oakmont, 1995 N.Y. Misc. LEXIS 229, at *1–2.

\textsuperscript{18} Id. at *10.

\textsuperscript{19} Id. at *13–14.

\textsuperscript{20} 47 U.S.C. § 230(a)(1).

\textsuperscript{21} 47 U.S.C. § 230(a)(2), (5).

\textsuperscript{22} See 47 U.S.C. § 230(a)(3).

vital to the internet because it gives companies “broad leeway to moderate discussions” in a manner that is best suited for their company. This has allowed website operators to host a large array of “user-generated content,” which spurred the rise of the social media industry and information platforms like Google and YouTube. Felix Gillette emphasized the importance of § 230 to the internet when he stated, “[i]t’s no hyperbole to call Section 230 the foundation on which the modern internet was built.” Section 230 was intended to promote the growth of internet companies, while protecting them from defamatory statements of third-party users on their sites. The courts have emphatically protected § 230's legislative intent to incentivize website operators to self-police the internet for obscene and offensive content, which has resulted in courts “almost always” granting immunity to website operators.

III. HOW COURTS HAVE INTERPRETED § 230

The United States Supreme Court has not taken up a case concerning how courts should interpret § 230. Courts have construed § 230 broadly because website operators that display third-party content can have an “infinite number of users generating an enormous amount of potentially harmful content.” If website operators were held liable for all harmful


25. Id.


29. See Reno v. ACLU, 521 U.S. 844 (1997). This was the only case the Supreme Court has addressed concerning the CDA, but it has not addressed § 230 of the CDA.

content on their sites, it would impose too great a burden on
website operators to screen every post made on their site.\(^\text{31}\) Courts have commonly held that “internet service providers, website exchange systems, online message boards, and search engines” fall within the “interactive computer service[s]” that § 230 intends to protect.\(^\text{32}\)

When interpreting the plain language of § 230, the statute creates a broad immunity against “any cause of action that would make service providers liable for information originating with a third-party user of the service.”\(^\text{33}\) Plaintiffs who bring lawsuits against website operators under § 230(c)(1) usually bring claims of defamation, negligence, or intentional infliction of emotional distress against the website operator.\(^\text{34}\) Congress expanded § 230 protection for website operators against state and local laws under § 230(e)(3) which says “[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.”\(^\text{35}\) The ultimate question courts consider in analyzing § 230(c)(1) as a defense is whether the website operator is to be considered a “speaker” of the content that is at issue, or whether the website operator is a “publisher” exercising its traditional publisher

---

129 F.3d 327, 331 (4th Cir. 1997)); see also Universal Commc’n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 419 (1st Cir. 2007) (explaining that “the difficulty of separating lawful from unlawful speech, and the relative lack of incentives to protect lawful speech,” are why the courts should “broadly construe” Section 230 immunity); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003) (describing the § 230(c) immunity as “quite robust”); Ben Ezra, Weinstein, & Co. v. Am. Online Inc., 206 F.3d 980, 986 (10th Cir. 2000) (explaining that providing immunity to “publisher liability” is essential for a company to exercise “editorial and self-regulatory functions” without endless liability).

31. Backpage.com, 817 F.3d at 18–19 (citing Zeran, 129 F.3d at 331).

32. FTC v. LeadClick Media, LLC, 838 F.3d 158, 174 (2d Cir. 2016).

33. Zeran, 129 F.3d at 330; see also Doe v. MySpace, Inc., 528 F.3d 413, 418 (5th Cir. 2008) (explaining that § 230(c)(1) provides “broad immunity” to website operators for “all claims stemming from their publication of information created by third parties”).

34. Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1101–03 (9th Cir. 2009).

35. 47 U.S.C. § 230(e)(3); see also Benjamin Edelman & Abbey Stemler, From the Digital to the Physical: Federal Limitations on Regulating Online Marketplaces, 56 HARV. J. ON LEGIS. 141, 176–77 (2019) (explaining that § 230(e)(3) provides a “preemption clause” with the intention to encourage state laws targeted at internet companies). Otherwise, Congress would have just relied on the Supremacy Clause of the Constitution. Id.
functions. The use of the term “publisher” in § 230 indicates Congress’ intention to “immunize service providers only from publisher liability.” For the website operator to be the “speaker” of content, it must “directly and ‘materially’ contribute[ ] to what made the content itself ‘unlawful.’” Circuit courts have adopted a distinction between “taking actions (traditional to publishers) that are necessary to the display of unwelcome and actionable content and, on the other hand, responsibility for what makes the displayed content illegal or actionable.” A website operator can also be considered a “developer” of the content of third parties, which subjects the website operator to the same amount of liability as the “speaker” of the content. The website operator can be considered the “developer” of the third-party content if it “encourages or advises users to provide the specific actionable content” that brings about the lawsuit.

In FTC v. LeadClick Media, LLC, the Court of Appeals for the Second Circuit concluded that LeadClick “developed” the third parties’ content by giving instructions to the third parties on how to use false advertising that encouraged consumers to purchase the third parties’ weight-loss products. In Fair Housing Council v. Roommates.com, LLC, the defendant website operator developed questions, answers, and a search mechanism that encouraged discrimination in the way people can search for roommates. The decisions in LeadClick and Roommates.com

---

36. See Backpage.com, 817 F.3d at 19 (citing Barnes, 570 F.3d at 1101–02).
37. Zeran, 129 F.3d at 332.
40. Force, 934 F.3d at 68; 47 U.S.C. § 230(f)(3) (“The term ‘information content provider’ means any person or entity that is responsible, in whole or in part, for the creation or development of information provided . . .”).
41. Force, 934 F.3d at 69; see FTC v. LeadClick Media, LLC, 838 F.3d 158, 176 (2d Cir. 2016); Roommates.com, LLC, 521 F.3d at 1172.
42. LeadClick Media, LLC, 838 F.3d at 176–77; see also Force, 934 F.3d at 69 (“LeadClick’s suggestions included adjusting weight-loss claims and providing legitimate-appearing news endorsements, [which] materially contribut[ed] to [the content’s] alleged unlawfulness.”).
43. Roommates.com, LLC, 521 F.3d at 1165–68, 1172. Roommates.com required users to provide protected characteristics, and the website hid some listings depending on the submissions. Id. at 1167.
have opened up a slim path for plaintiffs to avoid § 230 barring their claim. An “interactive computer service” may apply § 230 protection “only with respect to information provided by another information content provider.” But if the “interactive computer service” is also an “information content provider,” then the website operator is “not immune from liability arising from publication of that content.”

Parties who claim harm by a website operator’s publication of third-party content still have a source of recourse if the “interactive computer service” is not also the “information content provider.” The party may sue the third-party user that generated the content, but not the website operator that enabled the third-party to publish the content online. Plaintiffs are hesitant to pursue a claim against the speaker of the content because the speaker may not have the financial resources to pay damages, and the identity of the speaker may not be readily apparent.

Unfortunately for plaintiffs, it is rare to find an interactive computer service that is also an information content provider. This leads to the dismissal of most § 230 cases. If the website operator is considered to be exercising its traditional publisher functions, the website operator is afforded immunity for the website operator’s “decisions with respect to that posting, but also for its inherent decisions about how to treat postings generally.” A website operator’s decisions in structuring its website, choosing what words and phrases can appear on the website, and deciding whether to “publish, withdraw, postpone, or alter content” are editorial choices that are considered

44. See LeadClick Media, LLC, 838 F.3d at 175; FTC v. Accusearch Inc., 570 F.3d 1187, 1197 (10th Cir. 2009).
45. Accusearch Inc., 570 F.3d at 1197 (quoting 47 U.S.C. § 230(c)(1)).
46. Id.; see 47 U.S.C. § 230(c)(1), (0)(2)–(3); Roomates.com, LLC, 521 F.3d at 1162 (9th Cir. 2008); Ben Ezra, Weinstein, & Co. v. Am. Online Inc., 206 F.3d 980, 985 (10th Cir. 2000).
47. See Doe v. MySpace, Inc., 528 F.3d 413, 419 (5th Cir. 2008); 47 U.S.C. § 230(c)(1), (0)(2)–(3).
48. See MySpace, Inc., 528 F.3d at 419.
49. Gillette, supra note 24 (“Section 230 cases frequently result in the spectacle of a tech giant squashing the complaints of users and smaller websites.”).
50. Doe v. Backpage.com, LLC, 817 F.3d 12, 20 (1st Cir. 2016) (quoting Universal Commc’n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 422 (1st Cir. 2007)).
“traditional publisher functions.” The website operator is generally only liable under § 230 if the party conducts “its own speech” on the website.

There was hope that courts would take a more critical stance towards § 230 when a more egregious group of bad actors, like “sites facilitating sex trafficking,” were involved. The case of Doe v. Backpage.com, LLC put a damper on these hopes.

In Doe v. Backpage.com, LLC, the plaintiffs alleged that Backpage.com (“Backpage”) acted with the intention to facilitate sex traffickers’ efforts to advertise victims of sex trafficking on their website, and that Backpage’s rules and processes governing advertisements made sex trafficking easier to conduct. The plaintiffs were victims of sex trafficking which resulted from advertisements posted on Backpage. The advertisements posted on Backpage included images of the particular plaintiffs, usually taken by the traffickers. As a result of the advertisements, the plaintiffs were raped numerous times; two of the plaintiffs were allegedly raped 1,000 and 900 times respectively by users of the website. The plaintiffs alleged that Backpage, “engaged in a course of conduct designed to facilitate sex traffickers’ efforts to advertise their victims on the website . . . [which] led to their victimization.

Backpage provided online advertising, and allowed users of its site to post advertisements of categories that relate to the user’s product or service that is being sold. It hosted more than


54. Id. at 453.

55. Backpage.com, LLC, 817 F.3d at 16.

56. Id. at 17.

57. Id. (noting that a small number of the photos were taken by the plaintiffs).

58. Id.

59. Id. at 16.

60. Id.
eighty percent of the online advertising for “illegal commercial sex in the United States.” 61 One of the categories on Backpage’s website was titled “Adult Entertainment,” which contained a subsection titled “Escorts.” 62 Backpage had an automated filtering system that screened out advertisements containing certain prohibited terms, such as “barely legal” and “high school,” but the person posting the advertisement could implement similar phrases, such as “brly legal” or “high schl” which would circumvent the filtering system. 63

The Court of Appeals for the First Circuit determined that Backpage was exercising traditional publisher functions. Backpage did not require phone or email verification for an account, nor the specific date, time, or location of the photographs in the advertisements, and Backpage’s rules allowed people to post in the future after they had entered a prohibited term in a previous post. 64 The plaintiffs acknowledged that the content of the advertisements were provided by either the traffickers, or the plaintiffs themselves, not Backpage. 65 Due to Backpage exercising traditional publisher functions, and not acting as the speaker of the content, § 230(c)(1) barred the plaintiffs’ claim. 66

Courts have also rejected claims seeking to hold website operators liable for “failing to provide sufficient protections to users from harmful content created by others.” 67 In Doe v. MySpace Incorporated, the plaintiffs sued MySpace Inc. (“MySpace”) alleging that MySpace failed to “implement basic safety measures to prevent sexual predators from communicating with minors on its web site.” 68 The plaintiff’s daughter was thirteen years old when she created a MySpace account. 69 The daughter lied on her Myspace profile and said that she was eighteen years old, which allowed her to evade the

---

61. Petition for Writ of Certiorari at 7, Backpage.com, LLC, 817 F.3d 12, (No. 16-276).
62. Backpage.com, LLC, 817 F.3d at 16.
63. Id. at 17.
64. Id. at 21.
65. Id. at 19.
66. Id. at 23–24.
67. Id. at 21.
68. Doe v. MySpace Inc., 528 F.3d 413, 416 (5th Cir. 2008).
69. Id.
safety features on the website and made her profile public. The daughter met a nineteen-year-old man on MySpace, and when the two met in person, the daughter was sexually assaulted by him.

The plaintiffs alleged that MySpace was not the publisher of the information, so § 230 would not protect MySpace from the plaintiffs' claims. They alleged that their claim was predicated solely on "MySpace’s failure to implement basic safety measures to protect minors." The district court and Fifth Circuit rejected the plaintiffs' argument, holding that if MySpace had not published communications and contact information of the daughter and the nineteen-year-old, the two would have never met. MySpace was afforded § 230 protection because it exercised traditional public functions, and the plaintiffs' claim was dismissed.

The Second Circuit applied a similar analysis when a plaintiff alleged that Grindr LLC, an online dating application, was “defectively designed and manufactured.” Plaintiff's ex-boyfriend “created Grindr profiles to impersonate [plaintiff],” and the ex-boyfriend directed other users on the application to plaintiff's home and workplace. The court concluded that the plaintiff's "ex-boyfriend’s online speech is precisely the basis of [plaintiff]'s] claims that Grindr is defective and dangerous,” and that this claim is based on “information provided by another information content provider.” Grindr was afforded § 230 immunity, and the court dismissed the plaintiff's claim.

Currently, as long as the material was created by a third-party and the website operator did not “materially contribute to

70. Id.
71. Id.
72. Id. at 419.
73. Id.
74. Id. at 419–20 (citing Doe v. MySpace Inc., 474 F. Supp. 2d 843, 849 (W.D. Tex. 2007)). In a similar 2002 case, the plaintiff argued that the defendant internet service provider failed to protect the user on its site, and the case was dismissed because it related to the defendant's “monitoring, screening, and deletion of content from its network,” which are traditional publisher functions. Green v. Am. Online, 318 F.3d 465, 471 (3d Cir. 2002).
75. MySpace Inc., 528 F.3d at 422.
77. Id.
78. Id. at 590.
79. Id. at 591.
its development,” a website operator is granted “broad immunity” from § 230(c)(1).\textsuperscript{80} As the courts have afforded website operators § 230(c)(1) protection in situations of sex trafficking, death threats, sexual abuse, and other gruesome acts, debate emerges over whether § 230 needs to be remedied, and if so, is Congress, the courts, or the public consumers the best group to bring about that change.

IV. SECTION 230(C)(2)'S GOAL TO ENCOURAGE CONTENT MONITORING, AND WHY IT FAILED

While there are frequent claims from individuals being harmed by the content displayed on a website, there are also claims from individuals when the website operator modifies or removes third-party’s content. Many individuals allege a deprivation of their free speech rights when a website operator modifies or removes their content from a site.\textsuperscript{81}

One goal of § 230 was to “encourage voluntary monitoring for offensive or obscene material” without fear of liability.\textsuperscript{82} The statute does not require website operators to filter offensive content,\textsuperscript{83} but states that website operators shall not be liable for “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.”\textsuperscript{84} The purpose of § 230(c)(2) is to provide internet companies a “safety net” with regards to filtering out content on their sites that the internet company deems to be offensive.\textsuperscript{85}

\textsuperscript{81} Ryan French, Comment, Picking Up the Pieces: Finding Unity After the Communications Decency Act Section 230 Jurisprudential Clash, 72 La. L. Rev. 443, 479 n.263 (2012).
\textsuperscript{82} Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1099–1100 (9th Cir. 2009) (citing Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1122 (9th Cir. 2003)); see also Olivier Sylvain, Intermediary Design Duties, 50 Conn. L. Rev. 203, 239 (2018) (“Section 230(c)(2)(A) encourages websites to keep objectionable content out without fear of liability for failing to do so well.”).
\textsuperscript{84} 47 U.S.C. § 230(c)(2)(A).
\textsuperscript{85} Doe v. GTE Corp., 347 F.3d 655, 659 (7th Cir. 2003).
Congress did not include every type of offensive speech in § 230(c)(2), so courts have inferred that Congress likely intended to provide forms of discouraged content that “Congress could not identify in the 1990s.” Congress intended to give website operators “tools to avoid not only violent or sexually explicit materials, but also harassing materials.” Courts have taken this to signify that “[s]pam, malware and adware could fairly be placed close enough to harassing materials to at least be called ‘otherwise objectionable.’”

A website operator has “unbridled discretion” under § 230(c)(2) to block the online material based on the content of the post, and not because of the “identity of the entity that produced it.” Website operators have “robust statutory immunity” under § 230(c)(2), allowing courts to adjudicate these cases in a more time and cost efficient manner and advance the courts’ interest in judicial economy. As long as the website operator exercised “good-faith efforts,” the website operator may screen and/or block third-party content.

Although § 230(c)(2) does provide “unbridled discretion,” website operators generally prefer to rely on § 230(c)(1) to defend their actions because § 230(c)(2) requires the website operator’s blocking and screening be made in “good faith.” “Plaintiffs always have incentives to contest the defendant’s good faith, which delays the court’s application of § 230(c)(2)’s immunity—and sometimes overcomes it.”

86. Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 938 F.3d 1026, 1037 (9th Cir. 2019).
87. Id.
88. Id.; see also Holomaxx Techs. v. Microsoft Corp., 783 F. Supp. 2d 1097, 1104–05 (N.D. Cal. 2011) (explaining that the challenger has to claim that the website operator acted in bad faith by removing the post); e360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605, 608 (N.D. Ill. 2008) (concluding that extreme deference to the website operator’s subjective determination is permissible).
89. Enigma Software Grp. USA, LLC, 938 F.3d at 1033.
91. Doe v. Backpage.com, LLC, 817 F.3d 12, 18 (1st Cir. 2016).
92. Enigma Software Grp. USA, LLC, 938 F.3d at 1036; see Eric Goldman, The Ten Most Important Section 230 Rulings, 20 TUL. J. TECH. & INTELL. PROP. 1, 6 (2017).
93. Goldman, supra note 92, at 6; see Goldman, supra note 90, at 671 (arguing that the “good faith” aspect of § 230(c)(2) should be removed because it increases the chances that both parties will accumulate high adjudication
These concerns have been contrasted with strong policy arguments for the value of § 230(c)(2). Eric Goldman, a Professor at the Santa Clara University School of Law, predicted two reasons why website operators will use § 230(c)(2) infrequently. Goldman argued that (1) website operators are reluctant to terminate customers from their sites because customers increase revenue for website operators; and (2) that website operators will be concerned with losing customer trust if they capriciously terminate accounts or remove posts. Website operators want leeway to shape their website in a way that will engage customers and promote the free expression of consumers, which is important for growth.

Websites need some “provider intervention” to protect website users from other users and to prevent security or technical concerns. An additional challenge to modifying or removing third-party content is that flagging the content on a website requires an ample amount of resources. The fear of being sued may cause online entrepreneurs to be hesitant in developing new applications, as they would have to “divert resources to defend the parade of lawsuits arising from illegal third-party conduct.”

Facebook has invested a lot of money into moderating content posted on its website, and its large investment has been insufficient in removing hate speech and misinformation from the platform. Facebook has 15,000 content moderators around the world who are responsible for reviewing “potentially objectionable content” and then making a decision as to whether costs just to reach a prevailing decision for the website operator).

94. Goldman, supra note 90, at 672.
95. Id. Goldman’s article referred specifically to terminating user accounts under § 230(c)(2), but Goldman’s application can be evaluated when looking at all actions website operators can take under § 230(c)(2).
96. See Gillette, supra note 24; Daphne Keller, The Stubborn, Misguided Myth that Internet Platforms Must Be ’Neutral,’ WASH. POST (July 29, 2019, 6:00 AM), https://www.washingtonpost.com/outlook/2019/07/29/stubborn-nonsensical-myth-that-internet-platforms-must-be-neutral/ (“If platforms couldn’t enforce content policies while retaining immunity, communications today would look a lot like they did in 1965. We could passively consume the carefully vetted content created by big companies like NBC, . . . but we wouldn’t have many options in between.”).
98. Sylvain, supra note 82, at 244.
the content can remain on Facebook. Content moderators have been described as the closest parallel to first responders, as they are often the “first line of defense for reporting and responding to various crimes playing out online.”

There are more than 100,000 content moderators in the world, with some estimates as high as 150,000.

In just her first day as a content moderator, one of the moderators learned the emotional challenges that come with the job, as she saw, among other things, “anti-Semitic speech, bestiality photos and video of what seemed to be a girl and boy told by an adult off-screen to have sexual contact with each other.” Content moderators can be fired after making only “a handful of errors a week” in deciding to remove the content or allow the content to remain on the website. They are also developing “PTSD-like symptoms.” Commenters note that, “[m]oderators cope with seeing traumatic images and videos by telling dark jokes about committing suicide, then smoking weed during breaks to numb their emotions.”


100. Benjamin Powers, The Human Cost of Monitoring the Internet, ROLLING STONE (Sept. 9, 2017, 1:00 PM), https://www.rollingstone.com/culture/culture-features/the-human-cost-of-monitoring-the-internet-202291/ (estimating that there are 150,000 content moderators as of 2017); see Casey Newton, What Tech Companies Should Do About Their Content Moderators’ PTSD, VERGE (Jan. 28, 2020, 6:00 AM), https://www.theverge.com/interface/2020/1/28/21082642/content-moderator-ptsd-facebook-youtube-accenture-solutions (“[C]ontent moderation is often a dead-end career.”).


103. Newton, supra note 100.

104. Id.

105. Id.; see Elizabeth Dwoskin, et al., Content Moderators at YouTube, Facebook and Twitter See the Worst of the Web—and Suffer Silently, WASH. POST (July 25, 2019, 1:00 PM), https://www.washingtonpost.com/technology/2019/07/25/social-media-companies-are-outsourcing-their-dirty-work-philippines-generation-workers-is-paying-price/ (stating that moderators are expected to maintain accuracy
sells its content moderation services to Facebook, YouTube, and Twitter, among others, requires employees to acknowledge that their work can lead to PTSD.”

Employing content moderators is a burdensome task for website operators that host large amounts of third-party content like Facebook and YouTube. If fewer users are engaging in their services because companies are restricting harmful speech, the value of their applications is reduced.

Not only is there a high turnover rate with content moderators, content moderators require a lot of investment and resources. Facebook has 15,000 content moderators who get paid at an average salary of $28,800, totaling $432 million in labor costs for content moderators. That does not include the cost of equipment, the cost of developing strategies for content moderation, or the indirect costs of employing content moderators, such as having therapists to help them better cope with the content they are viewing. Although Facebook invests a lot of capital to monitor its platform, there is still a lot more Facebook needs to do to combat misinformation and hate speech, given the amount of people that use Facebook and rely on it to obtain news.

---

106. Newton, supra note 100.
107. Sylvain, supra note 82, at 244.
109. Newton, supra note 100; see Rob Copeland & Tripp Mickle, *Silicon Valley Was First to Send Workers Home. It’s Been Messy.*, WALL ST. J. (Mar. 14, 2020, 9:00 AM), https://www.wsj.com/articles/silicon-valley-was-first-to-send-workers-home-its-been-messy-11584190800?mod=business_lead_pos10 (stating that during the COVID-19 outbreak, Facebook recommended its employees remain at home when feasible). But Facebook required content moderators reviewing posts of urgent danger, “such as the policing of videos or images related to child abuse or pornography,” to remain at the office. Id.
111. See Deepa Seetharaman, *QAnon Booms on Facebook as Conspiracy Group Gains Mainstream Traction*, WALL ST. J. (Aug. 13, 2020, 9:10 PM), https://www.wsj.com/articles/qanon-booms-on-facebook-as-conspiracy-group-gains-mainstream-traction-11597367457 (noting that “Facebook groups have been central to building the QAnon network,” which is known for embracing many debunked conspiracy theories); Lukas I. Alpert, *Coronavirus Misinformation Spreads on Facebook, Watchdog Says*, WALL ST. J. (Apr. 20, 2020, 10:29 PM), https://www.wsj.com/articles/coronavirus-misinformation-
Content moderators have proven to help make websites safer, but content moderators will need a healthier work environment to prevent high employee turnover and emotional issues that result from the job. Content moderators need to be informed, before accepting the position, of the emotional challenges that come with the job. Companies also need to ensure strong mental health programs for content moderators and incorporate rotation programs for the content moderators to limit exposure to traumatic content in intermittent periods. These investments will require substantial capital, but to sustain content moderation, website operators must promote a healthy work environment for content moderators.

In September 2018, Twitter attempted to enact a policy similar to Facebook’s. Twitter will use artificial intelligence to combat speech that violates its policies, and users can report offensive tweets, but “the suspect tweets will always be reviewed by a human.” Twitter has only 1,500 content moderators, compared to around 15,000 content moderators at Facebook. Twitter leaves dangerous content on its site instead of removing it by filtering to make the content not “immediately visible to a

---


113. Id.

114. Id.

115. Sara Harrison, Twitter and Instagram Unveil New Ways to Combat Hate—Again, WIRED (July 11, 2019, 7:00 AM), https://www.wired.com/story/twitter-instagram-unveil-new-ways-combat-hate-again/.

116. Id.

user.”\textsuperscript{118} Twitter has asserted that it wants to create a safer website, but the measures Twitter has put in place have not achieved its objectives. Twitter has ignored the advice of scholars who have asked to help mitigate offensive speech on their platform.\textsuperscript{119} During the period of January 2019 through June 2019, 11,757 million accounts were reported for harmful content on Twitter.\textsuperscript{120}

The amount of content on these websites illustrates why these companies need § 230 immunity:

According to the social media intelligence firm Brandwatch, there are about 3.2 billion images shared each day. On Youtube there are 300 hours of video uploaded every minute. On Twitter, 500 million tweets are sent each day, which amounts to about 6,000 Tweets each second. If two percent of the images uploaded daily are inappropriate, that means that on any given day, there may [be] 64 million posts that violate a terms of service agreement alone.\textsuperscript{121}

This high volume of content shows the pressure facing website operators and the breadth of liability that website operators would be subject to without § 230 immunity. Facebook and other large website operators have the resources to invest in content moderators, but most other smaller website operators are struggling to achieve profitability and do not have the resources to invest in modifying and removing offensive speech on their websites.\textsuperscript{122}

\textsuperscript{118} Id.
\textsuperscript{120} Id. (finding that during the January–June 2019 period, 4,551 million accounts were reported for harmful conduct about abuse, 5,202 million accounts were reported for posting hateful conduct, and 2,004 million accounts were reported for posting violent threats on Twitter).
\textsuperscript{121} Powers, supra note 100.
V. The Criticism Offered Towards § 230

There are benefits that § 230 has advanced, which Congress has pointed out, but there are flaws with § 230 that need to be considered. The district court in *Blumenthal v. Drudge* expressed concern about § 230 when it said:

> If it were writing on a clean slate, this Court would agree with plaintiffs. [A website operator] has certain editorial rights with respect to the content provided by [the third party] and disseminated by [the website operator], including the right to require changes in content and to remove it; . . . [b]ecause [a website operator] has the right to exercise editorial control over those with whom it contracts and whose words it disseminates, it would seem only fair to hold [the website operator] to the liability standards applied to a publisher or, at least, like a book store owner or a library, to the liability standards applied to a distributor.\(^\text{123}\)

The concern with content monitoring is that the guidelines for how to monitor the content of its users should be set by the legislature.\(^\text{124}\) The court in *Blumenthal* emphasized this concern when stating that companies should be responsible for monitoring users’ content, but they must oblige the legislative intent in § 230.\(^\text{125}\) Right now, the responsibility is up to website operators to initiate their own policies. But if “all of the ‘big five’


\(^\text{125}\) *Blumenthal*, 992 F. Supp. at 52.
tech [companies]-Apple, Amazon, Facebook, Microsoft, and Alphabet . . . adopted a joint policy to suppress hate speech wherever they can,” we would be leaving “such a complex and momentous social decision to the boards of . . . private corporations clustered in the San Francisco and Seattle metropolitan areas.”

The legislature has provided increased criticism towards § 230, with both political parties having negative sentiment towards the statute. Republican members of Congress have asserted that website operators have “suppress[ed] their viewpoints, arguing that the spirit of Section 230 is predicated on companies remaining politically neutral.” Democrats, on the other hand, express concern that tech companies often rely on § 230 “to ignore the collateral damage of their users’ bad behavior.”

Even the former United States Attorney General, William Barr, has criticized § 230, although he said that the United States Department of Justice has not declared a position on the law. Attorney General Barr said, “[t]he early days of online public bulletin boards . . . have been replaced by platforms with sophisticated content moderation tools, algorithms, recommendation features, and targeting. With these new tools, the line between passively hosting third-party speech and actively curating or promoting speech starts to blur.”

President Trump has been critical of social media companies flagging or removing speech by third-party users on their platforms when that speech violates the company’s policies.

126. Langvardt, supra note 124, at 1385.
127. See Gillette, supra note 24.
130. See William P. Barr, Attorney General Dep’t of Justice, Opening Remarks at the DOJ Workshop on Section 230: Nurturing Innovation or Fostering Unaccountability? (Feb. 19, 2020).
131. Id.
On May 28, 2020, President Trump issued an “Executive Order on Preventing Online Censorship,” arguing that social media companies have not acted in “good faith” in removing third-party content, and a company that removes third-party content in bad faith should lose its protection under § 230(c)(2). The Executive Order asks, among other things, the Federal Communications Commission (“FCC”) to declare what actions constitute restricting speech “in good faith,” in an attempt to limit the authority of website operators to moderate their own platforms.

Legal experts assert that the Executive Order is “toothless in terms of enforcement.” In general, the First Amendment “prohibits only governmental abridgment of speech.” The First Amendment does not apply to private entities when the private entity is providing a forum for speech, “because the private entity is not a state actor.” The FCC emphasized that President Trump’s Executive Order has no impact on website operators, stating that “the First Amendment and Section 230 remain the law of the land and control here.” While we have yet to see substantive changes to § 230, Democrats and Republicans have both addressed discontent with the law, marking a warning to website operators that change may be on the horizon.

Some critics have suggested that “notice-based liability” would be a proper responsibility for website operators to
“Notice-based liability” would impose liability on website operators for “third-party defamatory content only on proof of notice and subsequent failure to remove the defamatory content within a reasonable time.” The Fourth Circuit, dissatisfied with a notice-based liability argument, said that notice of a “potentially defamatory posting” thrusts the website operator “into the role of a traditional publisher.” The “traditional editorial functions” are exactly what § 230 is intended to protect. An additional issue with “notice-based liability” is that it does not prevent the harm from the third-party content of being enacted. Content moderators must determine whether the third-party content should be removed before more users see the content, but this is after the content has already been on the website for users to see.

With “notice-based liability,” the damage would already be done by the time content moderators review the content, and the website operator would feel forced to remove the content out of concern for defamation liability. It would be impossible for “notice-based liability” to be applied equally because website operators have different amounts of resources to allocate to content monitoring. The companies that do not have the resources to invest in content monitoring would receive notice of the third-party content too late, making them unable to mitigate the damage. The companies that do have the resources to invest in content monitoring would be subject to defamation and free speech liability every time a content moderator makes a decision to remove the content.

141. Id. at 1507.
143. Id. at 330 (“[L]awsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content—are barred.”).
144. See Queenie Wong, Facebook Content Moderation Is an Ugly Business. Here’s Who Does It, CNET (June 19, 2019, 12:53 PM), https://www.cnet.com/news/facebook-content-moderation-is-an-ugly-business-heres-who-does-it/ (explaining that the content has already been on the website before content moderators must decide to allow or remove the post).
145. See Susan Freiwald, Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation, 14 HARV. J.L. & TECH. 569, 640–41 (2001) (noting that “notice-based liability” would lead to a reduced level of online speech, and First Amendment concerns as website operators would “find it easier just to remove the posting rather than investigate”).
to permit or remove a post, which raises the concern of endless litigation that the legislature and courts feared.\footnote{146}{See Zeran, 129 F.3d at 331 (“Interactive computer services have millions of users . . . [and] [t]he specter of tort liability . . . would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems.”).}

The criticism towards § 230 emerges from our innovative technology sector. The United States is very innovative; our technology and economy grow at a much faster rate than our legal system can keep up with.\footnote{147}{Julia Griffith, A Losing Game: The Law Is Struggling to Keep Up with Technology, J. HIGH TECH. L. (Apr. 12, 2019), https://sites.suffolk.edu/jhtl/2019/04/12/a-losing-game-the-law-is-struggling-to-keep-up-with-technology/ (“Technology seems to be advancing at a rate that the law simply cannot keep up with. It has been estimated that the law is at least five years behind developing a technology.”).} Innovation in the technology sector illustrates not only that website operators need § 230, but public citizens need it as well because the customs of public citizens adapt to advances in technology. Individuals “love what Section 230 does for them,”\footnote{148}{Wiener, supra note 128.} and politicians think of § 230 as a Facebook and Twitter problem instead of looking at the internet in totality. Website operators that rely on generating content from third-party users (i.e., Yelp, Reddit, etc.) would be crushed without the protection of § 230,\footnote{149}{Id.} disrupting the innovation developed through many website operators on the internet.

A 2019 Pew Research Report showed that fifty-five percent of Americans get their news from social media “either ‘often’ or ‘sometimes,’” an eight percent increase from 2018.\footnote{150}{Peter Suciu, More Americans Are Getting Their News from Social Media, FORBES (Oct. 11, 2019, 10:35 AM), https://www.forbes.com/sites/petersuciu/2019/10/11/more-americans-are-getting-their-news-from-social-media/#6b7b60673e17; see also 47 U.S.C. § 230(a)(5) (“Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.”).} As social media becomes more important in relaying news to the public, the public expects more content moderation in regulating disinformation on websites.\footnote{151}{Carys Afoko, Government Can’t Regulate Facebook – It’s Up to All of Us, GUARDIAN (Apr. 1, 2019, 2:00 PM), https://www.theguardian.com/commentisfree/2019/apr/01/government-regulate-facebook-mark-zuckerberg-social-media.} Most news sources do not receive § 230 immunity.\footnote{152}{See Blumenthal v. Drudge, 992 F. Supp. 44, 51 (D.D.C. 1998) (noting...
of conveying the news, the public wants them to take a more proactive approach in flagging misinformation and ensuring that the news conveyed is informative. But social media was founded on connecting people all around the world. The evolution of social media into a news outlet for most Americans is a new responsibility. Social media companies are again fearing the consequence of restricting free speech and the limits of their § 230 immunity.¹⁵³

VI. THE SOLUTION: MAINTAIN § 230, BUT RESOLVE THIS INTERNET PROBLEM THROUGH TAX CREDITS

The Court of Appeals for the First Circuit emphasized the financial and legal problems that will arise to website operators by making them responsible for content that third parties post on their websites.¹⁵⁴ The Court of Appeals for the Fourth Circuit recognized the burden placed on website operators by imposing the need to monitor content by stating, “[i]t would be impossible for service providers to screen each of their millions of postings for possible problems.”¹⁵⁵ These challenges are compounded by the fact that only seventeen percent of tech companies are profitable, and most of them do not have the cash on hand to devote to monitoring content and to finance substantial increases in legal costs.¹⁵⁶ If Congress ends or limits § 230 protection for website operators, it could significantly reduce the topics discussed on the internet, as well as the number of users speaking on websites.¹⁵⁷ Legal experts have echoed the negative financial impact that revoking § 230 would have on website operators in asserting:

---

¹⁵³. See generally The Impact of Social Media: Is it Irreplaceable?, WHARTON (July 26, 2019), https://knowledge.wharton.upenn.edu/article/impact-of-social-media/ (“[S]ocial media . . . continues to evolve at lightning speed, making it tricky to predict which way it will morph next.”).

¹⁵⁴. Doe v. Backpage.com, LLC, 817 F.3d 12, 18–19 (1st Cir. 2016); see also Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).

¹⁵⁵. Zeran, 129 F.3d at 331 (explaining that website operators would feel pressured to “severely restrict the number and type” of content posted on sites if not afforded § 230 immunity).

¹⁵⁶. Lee, supra note 122.

¹⁵⁷. Goldman, supra note 90, at 671.
Without Section 230, only platforms with the resources for constant litigation would survive; even there, user-generated content would be heavily restricted in service of diminished liability. Social-media startups might fade away, along with niche political sites, birding message boards, classifieds, restaurant reviews, support-group forums, and comments sections. In their place would be a desiccated, sanitized, corporate Internet—less like an electronic frontier than a well-patrolled office park.\footnote{158. Wiener, supra note 128.}

Limiting or removing § 230 is not the solution; Congress needs to incentivize website operators to invest in monitoring third-party content on its websites through a tax credit.\footnote{159. Patrick J. Lipaj, Opportunity in Ohio: Rethinking Northeast Ohio’s Opportunity Zones with Local Legislation, 68 CLEV. ST. L. REV. 835, 852 (2020) (citation omitted) (“Tax credits offset the amount of tax due, meaning that a $1 tax credit saves $1 in tax for taxpayers in every tax bracket on their gross income.”).} Website operators are generally not the creators of the harmful messages on their websites, but intermediaries in publishing the posts.\footnote{160. See Doe v. Internet Brands, Inc., 824 F.3d 846, 852 (9th Cir. 2016) (citing Delfino v. Agilent Techs., Inc., 52 Cal. Rptr. 3d 376, 387 (Cal. Ct. App. 2006)).} In serving as intermediaries, website operators should be encouraged to take part in the solution, not be scared with the threat of liability.

Large companies that are investing in initiatives to reduce harmful content on their websites are seeing positive results.\footnote{161. Elizabeth Schulze, EU Says Facebook, Google, and Twitter Are Getting Faster at Removing Hate Speech Online, CNBC (Feb. 4, 2019, 12:07 PM), https://www.cnbc.com/2019/02/04/facebook-google-and-twitter-are-getting-faster-at-removing-hate-speech-online-eu-finds-.html.} The European Union reported that Facebook, Google, Instagram, Twitter, and YouTube removed an average of seventy-two percent of hate speech on their platforms during 2018, and eighty-nine percent of “content flagged as hate speech was reviewed by [these companies] within 24 hours, up from 40 percent in 2016.”\footnote{162. Id. In 2016, these companies only removed twenty-eight percent of}
intelligence and algorithms to detect hateful speech on their websites.\footnote{163} While these initiatives are not going to completely eliminate dangerous content on these websites, they help reduce offensive speech online.\footnote{164} We must encourage all companies to take these actions, and the best way to get companies that do not have the capital to invest in content monitoring to take part is for Congress to provide tax incentives.

Investing in content monitoring requires an immense amount of capital. Facebook has 15,000 content moderators, and Google has 10,000 employees working to mitigate hate speech on its platform.\footnote{165} When these companies include the costs of building and maintaining the artificial intelligence to monitor hateful content, the costs become significant.\footnote{166} This is an unreasonable task to ask every website operator to invest in hate speech on its platform. \footnote{Id. Facebook and Instagram have removed 82.4% and 70.6% of hate speech respectively; Google and YouTube have removed 80.0% and 85.4% respectively; Twitter has removed 43.5%. \footnote{Id.; see also Billy Perrigo, Facebook Says It’s Removing More Hate Speech than Ever Before. But There’s a Catch., TIME (Nov. 27, 2019, 4:42 AM), https://time.com/5739688/facebook-hate-speech-languages/ (“Facebook removed more than seven million instances of hate speech in the third quarter of 2019, . . . an increase of 59% [from] the previous quarter.”).}

\footnote{163. Perrigo, supra note 162 (“Facebook [can] now automatically detect 80% of hateful posts without needing a user to have reported them first.”); see also Seetharaman, supra note 119 (explaining that Twitter has discussed initiatives to use artificial intelligence to detect hateful speech, but these efforts have not come to fruition).}

\footnote{164. Perrigo, supra note 162 (explaining that Facebook’s algorithm covers around forty languages, leaving hateful speech in the many other languages undiscovered by the algorithm); see also Shirin Ghaffary, The Algorithms that Detect Hate Speech Online Are Biased Against Black People, VOX (Aug. 15, 2019, 11:00 AM), https://www.vox.com/recode/2019/8/15/20806384/social-media-hate-speech-bias-black-african-american-facebook-twitter (discussing a study finding that artificial intelligence models for processing hate speech were one-and-a-half times more likely to detect and flag tweets as hateful when written by African Americans). “[The models were] 2.2 times more likely to flag tweets written in African American English (which is commonly spoken by black people in the US).” \footnote{Id.}

\footnote{165. Newton, supra note 100; Schulze, supra note 161; Perrigo, supra note 162 (adding that Facebook has content moderators working “24 hours a day, seven days a week”).}

\footnote{166. These large companies have not disclosed the costs of their algorithms intended to remove hate speech. See Kirsten Grind et al., How Google Interferes with Its Search Algorithms and Changes Your Results, WALL ST. J. (Nov. 15, 2019, 8:15 AM), https://www.wsj.com/articles/how-google-interferes-with-its-search-algorithms-and-changes-your-results-11573823753 (noting that Google rarely releases information on its algorithms).}
without Congress providing some assistance.

Critics may argue that we should not be using the Internal Revenue Code (“IRC”) as a solution to make platforms safer. They argue that the IRC “should not be used for social policy purposes,” but rather social policies should be funded directly and openly by the government. But the tax code has been used many times by the federal and state governments to directly impact specific industries, and a tax credit has the same financial impact as direct funding from the government while also being easier legislation to enact.

In 1992, Congress enacted The Renewable Electricity Production Tax Credit (“PTC”), which today allows energy companies a tax credit “for electricity generated using qualified energy resources.” The PTC amounts to the product of “1.5 cents, multiplied by . . . the kilowatt hours of electricity . . . produced by the taxpayer . . . from qualified energy resources . . . that are sold by the taxpayer to an unrelated person during the taxable year.” The primary reason for originally enacting these tax subsidies was to encourage the United States to become more energy independent and competitive with fossil fuels as the United States was importing a lot of its oil supply. Congress also believed that the PTC was important to benefit the public as the PTC would contribute to reduce greenhouse emissions and pollution, which would benefit “society as a

167. Jay P. Kesan & Rajiv C. Shah, Shaping Code, 18 HARV. J.L. & TECH. 319, 382 (2005) (explaining that, among other concerns, an objection that critics raise to using “tax expenditures” being implemented to advance economic issues is that the “tax expenditures will place too high of an administrative burden on the IRS”).

168. Id. (citing Bernard Wolfman, Federal Tax Policy and the Support of Science, 114 U. PA. L. REV. 171 (1965)) (making the argument that direct subsidies to individuals and entities are a better solution than through tax expenditures).


171. I.R.C. § 45(a)(1)–(2).

While a tax break for website operators hosting third-party content would have the objective of improving the industry, it would also provide a benefit to the public by creating a safer environment on the internet.

When policies benefit the public as a whole, those policies will look to be incorporated globally. More than fifty percent of the world’s “renewable energy subsidies” are provided by countries in the European Union (“EU”), and other countries such as Canada, Japan, Australia, Israel, China, and India have invested in renewable energy subsidies. Content moderation has also seen a global response, illustrating the global mission to mitigate online harmful content. In 2016, the EU enacted a “Code of Conduct on countering illegal hate speech online” with Facebook, Microsoft, Twitter, and YouTube, which encouraged these companies to flag illegal hate speech and dispose of it in an appropriate time frame. By the end of 2018, most of these companies saw significant progress in flagging and removing hateful content; Google, Instagram, Snapchat, and Dailymotion decided to join the Code of Conduct in 2018. The EU’s action helps show that content moderation is a global issue and that advancements in content moderation will benefit the public. The companies that joined the Code of Conduct (besides Dailymotion) are worth billions of dollars, illustrating that it is more difficult for smaller companies to invest in content moderation.

We have also seen vital tax credits aimed at increasing research and development (“R&D”) expenses across all industries. The Research Tax Credit seeks to “encourage[]

176. Ana Garcia Valdivia, EU and IT Companies Make Significant Progress Against Illegal Hate Speech Online, Forbes (Feb. 5, 2019, 8:50 AM), https://www.forbes.com/sites/anagarcivaldivia/2019/02/05/eu-and-it-companies-make-significant-progress-against-illegal-hate-speech-online/#1a9d2a97379a.
177. Gary Guenther, Cong. Rsch. Serv., RL31181, Research Tax

https://digitalcommons.pace.edu/plr/vol41/iss1/7
business[es] to invest more in R&D than they otherwise would and reduces the tax burden on industries that require high amounts of R&D costs to get their product to market.\textsuperscript{179} The IRC provides an R&D tax credit for any “qualified research expenses,” allowing companies to receive a tax credit for around twenty percent of R&D expenses.\textsuperscript{180}

R&D tax credits have been crucial to industries that require a lot of capital investment, like the pharmaceutical industry.\textsuperscript{181} Estimates suggest that the cost of a pharmaceutical manufacturer to develop a new drug is “between $150 to $240 million,” with an additional $300 million more needed for “post approval research.”\textsuperscript{182} The high amount of capital investment for pharmaceutical companies comes with the risk that “[a]bout 85% of drug research projects fail before they are tested in human clinical trials.”\textsuperscript{183} Investing in content moderation will not require the same amount of capital investment as industries like the pharmaceutical industry, but the investment will be a huge financial burden for website operators and will require trial and error to develop strong algorithms and a healthy work environment for content moderators. Tax credits “have long been used to support technological development,”\textsuperscript{184} and Congress should welcome the opportunity to be a part of the solution to a safer internet.

A tax incentive for website operators is not a permanent solution. The objective would be for the legislature to help website operators manage the initial costs of content moderation, and once website operators have properly

\textsuperscript{178} Id.

\textsuperscript{179} Aaron S. Kesselheim et al., \textit{Pharmaceutical Policy in the United States in 2019: An Overview of the Landscape and Avenues for Improvement}, 30 STAN. L. \\ & POL’Y REV. 421, 428–29 (2019) (noting that it can cost a pharmaceutical company approximately $2.6 billion to develop a new drug, and the tax credit for R&D assists in managing the high amount of capital investment).

\textsuperscript{180} I.R.C §§ 41(a), 174. Section 174 provides that R&D “paid or incurred . . . during the taxable year in connection with [taxpayer’s] trade or business as expenses,” rather than capital expenses are to be treated as a deduction instead of a tax credit. \textit{Id.}

\textsuperscript{181} Id. at 429–30.

\textsuperscript{182} Id. at 429.

\textsuperscript{183} Id. at 430.

\textsuperscript{184} Kesan & Shah, \textit{supra} note 167, at 383.
incorporated the costs of content moderation into their budgets, then the companies would no longer need the tax credit. While the PTC has been great for renewable energy globally, there is growing concern that no one would invest in wind and solar energy in the United States without the benefit of tax credits.\footnote{See Matthews, supra note 172; Michael Bastasch, Warren Buffett: I Build Wind Turbines to Lower My Corporate Taxes, \textsc{Daily Caller} (May 6, 2014, 2:55 PM), https://dailycaller.com/2014/05/06/warren-buffett-i-build-wind-turbines-to-lower-my-corporate-taxes/ (explaining that Berkshire Hathaway and other companies Warren Buffett owns invest in wind turbines for the purpose of obtaining a tax credit).} A tax incentive is essential for website operators as they make initial capital investment into content moderation,\footnote{See O’Shea, supra note 112 (suggesting that artificial intelligence is an excellent tool to flag and remove harmful content, but content moderators are also needed to flag and remove the content that is challenging for artificial intelligence to detect).} and once they learn how to consistently incorporate these costs into their income statements, the website operators would hopefully not need the tax credit.

Website operators will need a tax credit to help mitigate the additional costs because they will face a learning curve in implementing content moderation strategies. Twitter explained in its 2018 Annual Report that as more users and content enters its site, it may become “increasingly difficult to maintain and improve the performance of [Twitter’s] products and services, . . . as [Twitter’s] products and services become more complex and user traffic increases.”\footnote{Twitter, Inc., Annual Report (Form 10-K) 23 (Feb. 20, 2019).} Twitter also acknowledged that it wants to target hate speech and spam accounts through launching algorithms, which will “require significant resources and time.”\footnote{Id. at 25; see also Microsoft Corp., Annual Report (Form 10-K) 24 (Aug. 1, 2019) (“Compliance with [online content] regulation[s] may involve significant costs or require changes in products or business practices that result in reduced revenue.”).} While Facebook has invested a lot in content moderation, not everything has gone smoothly.\footnote{Ghaffary, supra note 164.} Patience is required to allow these companies to find what content moderation strategy is best for them. These companies are helping the economy by investing “significant resources and time,”\footnote{Twitter, Inc., Annual Report (Form 10-K) 25 (Feb. 20, 2019).} and we need to encourage them to experiment and come up with a solution they think is best. A tax credit will prevent
these companies from rushing an unequipped solution, and it will provide the financial assurance to develop content moderation systems designed to have long-term success.

While a tax incentive for website operators to invest in content moderation will entice investment in the short-term, long-term success in content moderation is dependent on companies accepting content moderation costs as regular operating costs. The solution and action by website operators will be more organic if they believe investing in content moderation is the right thing to do, versus investing to receive a tax credit.191 Some companies may not invest in content moderation, but if the majority of website operators invest in assets that mitigate dangerous content on their websites, then laggards that are not investing in content moderation will be encouraged to invest as a matter of public policy.

VII. Why a Tax Credit is a Better Solution than a Direct Subsidy or Tax Deduction

Congress can create business development through multiple types of tax and funding initiatives.192 The legislature has, among other things, provided direct subsidies to industries, offered tax deductions to industries, and offered tax credits to industries. Direct subsidies would fulfill a similar goal to the tax credit by getting money directly to website operators, but it would face more difficult political challenges than a tax credit193 because tax credits have “much lower visibility than a direct spending program . . . [and the credit is] hidden in the tax code.”194

As tax law can be difficult for the public to understand, most politicians avoid political backlash for their votes on tax

---

191. See O’Shea, supra note 112 (explaining that the companies that invest enough to establish strong artificial intelligence and a healthy environment for content moderators will be in the best position to have a safe website for users).

192. Kesan & Shah, supra note 167, at 380–81 (“Commonly, justifications of government intervention are based on a form of market failure.”).

193. Id.

194. Id. at 381 (“[A] tax expenditure is still government spending; virtually any tax expenditure provision could be rewritten in the form of a direct spending program.”).
Dan T. Coenen explained the benefit to politicians of the difficulty of tax law to understand by stating:

Most people view tax structures (especially tax structures applicable to corporations and other businesses) as an esoteric specialty beyond their capabilities and willingness to understand. A failure to understand breeds a failure to second-guess, and a failure to second-guess implies that tax structures will, more readily than monetary subsidies, escape political opposition.

A subsidy for website operators to incentivize investment in content moderation could generate a negative viewpoint as the public may not like Facebook and other billion-dollar corporations receiving direct subsidies from taxpayer dollars. Politicians will face less risk pursuing a tax credit, and with both political parties expressing interest in improving § 230, a tax credit is politically safer than a direct subsidy.

Tax deductions as a solution for website operators would also be insufficient, as it would not provide enough of an incentive for website operators to invest in content moderation. A company may deduct any “ordinary and necessary expenses paid or incurred during the taxable year in carrying on any trade or business.” Companies list content moderation costs under “Operating Expenses,” as R&D, until the content moderation system is fully implemented, where it would then be part of the “cost of revenue.” A company can deduct these expenses from

196. Id.
197. Id. at 993 (“Subsidies may be looked upon more unfavorably because they are symptomatic of large and meddlesome government, while tax exemptions seem to comport with limited government and the value of private initiative.”).
198. See id. at 994; Kesel & Shah, supra note 167, at 381 (citation omitted) (“[M]any politicians who regard themselves as fiscally conservative would rather use a tax expenditure than support another ‘big government spending program’ — a key component to the popularity of tax expenditures.”).
199. See Gillette, supra note 24.
its net income as an “ordinary and necessary [business] expense,” and they should be able to keep deducting content moderation expenses, but an additional tax credit will lift a huge financial burden off of these companies. Twitter and Microsoft acknowledged that investing in content moderation will require “significant costs” and time and may also lead to a reduction in revenues for website operators. We want to incentivize investment in content moderation, not intimidate website operators with overwhelming costs.

In this hypothetical example, Company A had $1,000 in revenue for the taxable year, and $100 in content moderation costs. If the content moderation costs are a tax deduction as an “ordinary and necessary expense,” Company A would deduct the $100 in content moderation costs from the $1,000 in revenue, resulting in the company having $900 for its adjusted gross income. Assuming there were no other possible deductions, Company A would have a Net Taxable Income of $900. If the hypothetical tax rate were twenty percent, Company A would have to pay $180 in taxes to the Internal Revenue Service (“IRS”).

If Company A’s content moderation costs were a tax credit, rather than a tax deduction, Company A would have no deductions, and $1,000 in Net Taxable Income. With the hypothetical tax rate of twenty percent, Company A would have a Gross Tax of $200. But as a tax credit, the content moderation costs would be subtracted from the Gross Tax, making it a dollar-for-dollar reduction in Company A’s tax bill. Therefore,

204. Assume for this example that there are no other expenses and deductions that need to be implemented.
205. I.R.C. § 162(a).
206. JOEL S. NEWMAN ET AL., FEDERAL INCOME TAXATION CASES, PROBLEMS, AND MATERIALS 4–6 (7th ed. 2019). The formula for calculating the tax bill owed to the IRS, in general, is: Gross Revenue minus Deductions equals Net Taxable Income. The Net Taxable Income multiplied by the applicable tax rate results in the Gross Tax. The Gross Tax minus Credits and Prepayments equals the amount owed to the IRS or the refund the taxpayer will receive. See id.
207. See id.
208. See Tina Orem, Tax Credits Save You More than Deductions: Here Are the Best Ones, USA TODAY (Mar. 28, 2017, 1:07 PM),
Company A’s $100 in content moderation costs would be subtracted from its Gross Tax of $200, leaving Company A with a tax bill of $100 due to the IRS. The content moderation costs as a tax deduction only reduced Company A’s tax bill by $20, but when used as a tax credit, Company A reduced its tax bill by $100. While tax credits are a “dollar-for-dollar reduction in your actual tax bill,” a deduction just lowers the taxable income.

Section 230 has maintained its importance mostly because of cost. The concerns over endless liability without § 230 continue, and now we must consider the resources companies will need to improve content moderation into the cost analysis. Section 230, in maintaining its present condition, will give companies time to implement their content moderation strategies, and a tax credit will help ensure the companies have capital to take on the investment. This would help companies avoid the question of whether to invest in content moderation because it is the right thing to do, or to maintain profitability.

VIII. CONCLUSION

Congress states that one of the many reasons it enacted § 230 was “to remove disincentives for the development and utilization of blocking and filtering technologies . . . to restrict . . . access to objectionable or inappropriate online material.” While removing disincentives benefits companies, we must prioritize creating incentives for these companies to invest the time and resources towards content moderation. Congress has

209. If there were no content moderation costs, Company A would have had a Net Taxable Income of $1,000. Company A’s Net Taxable Income multiplied by the hypothetical twenty percent tax rate would have imposed a $200 tax bill on Company A.

210. Orem, supra note 208.

211. Airbnb, Inc. v. City of Bos., 386 F. Supp. 3d 113, 122 (D. Mass. 2019) (citing Doe v. Backpage.com, LLC, 817 F.3d 12, 18 (1st Cir. 2016)) (“Congress[] desire [was] to ‘allow[] website operators to engage in blocking and screening of third-party content, free from liability for such good-faith efforts.’”).

212. See Twitter, Inc., Annual Report (Form 10-K) 25 (Feb. 20, 2019) (noting that the company will need to devote a significant amount of time and resources to implement a strong content moderation strategy).

been known to lag in regulating the private sector. That must change. There is a common goal between Congress, companies, and the public to make websites safer. If Congress enacts a tax credit for companies that invest in content moderation, that benefit will spur investment in content moderation, which will help establish a safer internet for the public. The times of scaring website operators with liability must end, and the solution must reside in collaboration.

214. Griffith, supra note 147 ("[T]he law is at least five years behind developing a technology.").