Suffolk Journal of Trial and Appellate Advocacy

Volume 26 | Issue 1 Article 13

1-1-2021

Internet Regulation—Second Circuit Follows Majority of Courts in Broad Application of Communications Decency Act Immunity—Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019)

Alison Eleey
Suffolk University Law School

INTERNET REGULATION—SECOND CIRCUIT FOLLOWS MAJORITY OF COURTS IN BROAD APPLICATION OF COMMUNICATIONS DECENCY ACT IMMUNITY—*FORCE V. FACEBOOK, INC.*, 934 F.3D 53 (2D CIR. 2019).

The Communications Decency Act ("CDA") regulates the content of technology companies, including social media platforms.[1] The CDA has come under immense scrutiny, particularly regarding social media's role in facilitating attacks by terrorist organizations.[2] In *Force v. Facebook, Inc.*,[3] the United States Court of Appeals for the Second Circuit decided whether the CDA provided Facebook with immunity from claims that Facebook provided a platform for the terrorist organization, Hamas, to carry out various attacks.[4] The court held that Facebook was considered a "publisher" for purposes of the CDA, and was therefore immune from liability.[5]

---

[1] *See* 47 U.S.C. § 230(c)(2) (2019) (providing immunity to computer-service providers who regulate certain content). The subsection of the statute states as follows:

> No provider or user of an interactive computer service shall be held liable on account of— (A) 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; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1) [subparagraph (A)].

Id.

[2] *See* Nicole Phe, Note, *Social Media Terror: Reevaluating Intermediary Liability Under the Communications Decency Act*, 51 SUFFOLK U. L. REV. 99, 99 (2018) (outlining claims of victims' families against social media companies). The lawsuits discussed in Phe's note include a widow who sued Twitter for providing "material support" to ISIS in carrying out an attack on her husband. *Id.* In another suit, a family sued Google for its role in aiding an ISIS attack in Paris that killed their relative. *Id*. They argued that Google "'knowingly permit[ed] terrorist group ISIS to use their social networks,' and enabl[ed] them to carry out various terror attacks." *Id.*

[3] 934 F.3d 53 (2d Cir. 2019).

[4] *See id.* at 57 (stating issue of case). "The principal question presented in this appeal is whether 47 U.S.C. § 230(c)(1), a provision enacted by the Communications Decency Act of 1996, shields Defendant-Appellee Facebook, Inc., from civil liability as to Plaintiffs-Appellants' federal anti-terrorism claims." *Id.*

[5] *See Force*, 934 F.3d at 68 (stating holding); *see also* 47 U.S.C. § 230 ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."); Phe, *supra* note 2, at 68 (stating court's conclusion). Plaintiffs' argued that Facebook was not a "publisher" under the CDA because Facebook developed "matchmaking" algorithms that connected users to content that is most likely to gain interest and engage them in the platform. Phe, *supra* note 2, at 65. The court rejected this

Hamas is a Palestinian terrorist organization that has committed thousands of attacks in Israel, including five attacks against Americans between 2014 and 2016.[6] During these attacks, Hamas terrorists kidnapped and killed a teenager walking home from school, drove a car into a crowd and killed a 3-month-old baby, and stabbed three victims.[7] Hamas operatives carried out all of these attacks.[8] Hamas used Facebook to encourage attacks, celebrate the success of these attacks, and propagate their political views.[9] The Plaintiffs in *Force*, therefore, claimed that Facebook enabled Hamas to carry out the terrorist attacks and should be held liable for their role in aiding such attacks.[10]

Facebook is an "online social network platform and communications service" where users join the network and populate their pages with their own content.[11] Facebook does not review the content its users post, however, it does have a department focused on anti-terrorism.[12] These "counterterrorism specialists" use various techniques to identify terrorist

---

argument, holding that based on both statutory interpretation and precedent, Facebook's matchmaking algorithm did not render it a non-publisher. Phe, *supra* note 2, at 66; Jeff Neuburger, *Facebook Shielded by CDA Immunity Against Federal Claims for Allowing Use of Its Platform by Terrorists*, PROSKAUER (Aug. 9, 2019), https://newmedialaw.proskauer.com/2019/08/09/facebook-shielded-by-cda-immunity-against-federal-claims-for-allowing-use-of-its-platform-by-terrorists/ (discussing outcome of *Force* decision and court's rejection of Plaintiffs' "matchmaking" argument).

[6] *See Force*, 934 F.3d at 57-58 (describing Hamas organization and its principal aims). "Hamas is a Palestinian Islamist organization centered in Gaza. It has been designated a foreign terrorist organization by the United States and Israel. Since it was formed in 1987, Hamas has conducted thousands of terrorist attacks against civilians in Israel." *Id.* at 57. *But see* Matthew Levitt, *Hamas from Cradle to Grave*, MIDDLE EAST Q., Winter 2004 at 3, (available at https://www.meforum.org/582/hamas-from-cradle-to-grave) (last visited Dec. 30, 2020) (recognizing opposing view of Hamas as "nationalist movement" promoting "social welfare").

[7] *See Force*, 934 F.3d at 57-58 (outlining attacks and identifying victims).

[8] *See id.* (reiterating Hamas operatives executed all attacks).

[9] *See id.* at 59 (describing Hamas use of Facebook to celebrate and promote attacks). For example, the attack that killed the baby "came after Hamas posts encouraged car-ramming attacks at light rail stations." *Id.* Additionally, Hamas supporters were able to view celebratory posts on Facebook for these attacks because Facebook "allegedly failed to remove the 'openly maintained' pages and associated content of certain Hamas leaders, spokesmen, and other members." *Id.* (citations omitted).

[10] *See id.* (stating Plaintiffs' claim that Facebook helped Hamas carry out their terrorist acts). "[P]laintiffs claim [that] Facebook enables Hamas 'to disseminate its messages directly to its intended audiences,' to 'carry out the essential communication components of [its] terror attacks . . . .'" *Id.* (citations omitted).

[11] *See id.* at 58 (setting out Facebook's business model and how it works as social media platform).

[12] *See Force*, 934 F.3d at 58 (explaining how Facebook does not review or screen users' content). "Facebook's terms of service specify that a user 'own[s] all of the content and information [the user] post[s] on Facebook, and [the user] can control how it is shared through [the user's] privacy and application settings.'" *Id.* (citations omitted).

activity and remove concerning posts to the best of their ability.[13] Nevertheless, Facebook is unable to identify and remove all terrorist activity on its platform.[14]

The Plaintiffs' first complaint alleged that Facebook was civilly liable under the Anti-Terrorism Act for aiding and abetting international terrorist activities.[15] The district court dismissed the Plaintiffs' first complaint under 47 U.S.C. § 230(c)(1) because the Plaintiffs treated Facebook as a publisher.[16] The Plaintiffs then filed an amended complaint that kept the original allegations, but added an additional claim that Facebook "concealed its alleged material support to Hamas."[17] However, the district court again denied their motion under 47 U.S.C. § 230(c)(1), to which the Plaintiffs appealed.[18] The Second Circuit Court affirmed the judgment of the

---

[13] *See id.* at 60-61 (explaining work and background of counter-terrorist specialists). Facebook's Community Standards states that it "'remove[s] content that expresses support or praise for groups, leaders, or individuals involved in,' inter alia, '[t]errorist activity.'" *Id.* at 60. (citations omitted). Facebook thus employs "academics, engineers, and former prosecutors and law enforcement officers" to respond to reported posts for terrorist activity and remove content that violates its issued standards. *Id.* at 61.

[14] *See id.* at 59 (noting that Facebook failed to remove all terrorist pages from its platform); *see also* Ryan Goodman, *Why Can't Facebook Take Down All Terrorist Content?*, NEWSWEEK (Jan. 17, 2018, 8:10 AM), https://www.newsweek.com/why-cant-facebook-take-down-all-terrorist-content-782598 ("Content that Facebook declared did not violate its Community Standards included a photo of hooded gunmen aiming their weapons in an urban neighborhood with the caption, 'We Will Attack you in Your Home.'")

[15] *See Force*, 934 F.3d at 61 (detailing procedural history and Plaintiffs first complaint).

> In their First Amended Complaint, Plaintiffs claimed that, under 18 U.S.C. § 2333, Facebook was civilly liable for aiding and abetting Hamas's acts of international terrorism; conspiring with Hamas in furtherance of acts of international terrorism; providing material support to terrorists; and providing material support to a designated foreign terrorist organization.

Id.

[16] *See* Force v. Facebook, Inc., 304 F. Supp. 3d 315, 318 (E.D.N.Y. 2018) (dismissing first complaint).

> Examining the myriad opinions considering the application of that law, the court concluded that each of Plaintiffs' claims and theories of liability sought to hold Facebook liable based on its role as the 'publisher or speaker' of social media content generated by Hamas and affiliated individuals, and so were barred by the defense afforded by Section 230.

Id.

[17] *See Force*, 934 F.3d at 62 (stating contents of Plaintiffs' proposed amended complaint).

[18] *See Force*, 304 F. Supp. at 332 (dismissing Plaintiffs' motion to file amended complaint with prejudice); *see also Force*, 934 F.3d at 62 (noting Plaintiffs' appealed district court dismissal).

lower court, and held that Facebook is a publisher and therefore immune under § 230(c)(1) of the CDA.[19]

Before the enactment of the CDA, common law regulated the internet and its liability for third parties.[20] This common-law-focused model forced courts to determine which category the internet service provider ("ISP") fell under, which resulted in conflicting decisions among various jurisdictions.[21] The courts found that either: (1) ISPs would not regulate any of their content for fear of liability, or (2) ISPs overcensored the internet, which in turn inhibited free speech.[22] In *Cubby, Inc. v. Compuserve, Inc*., the district court held that a computer-database owner was a distributor, and therefore not liable for a third party's defamatory statements because they neither knew nor had reason to know about the statements.[23] A few years later, in a case with facts similar to *Cubby*, the court in *Stratton Oakmont v. Prodigy Servs. Co.* held that an online service provider was lia-

---

[19] *See Force*, 934 F.3d at 57 (affirming lower court's judgement).

[20] *See* Phe, *supra* note 2, at 102 (explaining legal history of internet service providers' liability prior to CDA). This "common law liability scheme consisted of three categories: primary publishers, distributors, and conduits." *Id.* These categories meant that liability varied depending on what category the party involved in the litigation fell under. *Id.* at 103.

> Under common law, primary publishers were held to the same standard of liability as original authors because they were in the best position to monitor and control content, and as a result, could have easily avoided or mitigated the harm caused by defamation. On the other hand, a distributor is liable for the distribution of a defamatory publication only if the distributor had actual or imputed knowledge of the defamation and failed to remove the defamatory post. Distributor liability hinged on the idea that even though distributors were not in a position to monitor and control content, they had the ability to minimize the harm of the defamation by refusing to sell or stock defamatory materials.

Id.

[21] *See id.* at 104 (explaining outcome of common-law-liability scheme). "As one court insightfully noted, 'more ideas and information are shared on the Internet than any other medium. But when we try to pin down this medium of exchange, we realize how slippery our notion of the Internet really is.'" *Id.*; *see also* Michelle Jee, *New Technology Merits New Interpretation: An Analysis of the Beadth of CDA Section 230 Immunity*, 13 HOUS. BUS. & TAX L.J. 178, 184 (2013) (noting increase in conficliting court decisions as internet expanded). As internet providers created forums where users could connect on the internet, "courts had conflicting views on how to adequately address claims against website operators for defamation." Jee, *supra* note 21, at 184.

[22] *See* Phe, *supra* note 2, at 106 (explaining Congressional issue with common-law liability).

[23] *See* 776 F. Supp. 135, 141 (S.D.N.Y. 1991) (finding "CompuServe, as a news distributor, may not be held liable if it neither knew nor had reason to know of the allegedly defamatory Rumorville statements, summary judgment in favor of CompuServe on the libel claim is granted."). CompuServe provides an online information service that individuals can subscribe to and gain access to information about thousands of sources within its electronic library. *Id.* at 137. The plaintiffs claimed that one of the sources on CompuServe's website published false statements about them and CompuServe failed to remove those statements. *Id.* at 138. However, the court found that CompuServe was a distributor and could not be held liable if they did not know or have reason to know about the defamatory statements. *Id.* at 141.

ble for a third party statement because it attempted to filter its content.[24] The conflicting holdings of these cases worried Congress, which led to the formation of the CDA.[25]

In 1996, Congress passed the CDA in an effort to "control and limit the exposure of children to indecent and obscene material online."[26] One year later, the Supreme Court struck down most of the CDA because it exposed internet providers to too much liability, which consequently prompted the addition of § 230.[27] Section 230 of the CDA provides immunity for internet providers who are treated as publishers of third-party content.[28] The purpose of this immunity was largely to continue the development of the internet and "to preserve the vibrant and competitive free market . . . for the Internet and other interactive computer services" without Federal or State regulation.[29] Moreover, there are three requirements for immunity

---

[24] *See* No. 31063/94, 1995 N.Y. Misc. LEXIS 229, at *13, 17 (N.Y. Sup. Ct. May 24, 1995) (holding Prodigy's "conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability than [the ISP in *Cubby*] and other computer networks that make no such choice."). The court found that Prodigy controlled its content because they were controlled by their members who, in turn, controlled the electronic bulletein boards on Prodigy's site. *Id.* at *9. Further, Prodigy had an automatic software that screened content. *Id.* Therefore, Prodigy was distinguished from the ISP in *Cubby* because Prodigy chose to regulate their content, thus opening them up to liability. *Id.*

[25] *See* Phe, *supra* note 2, at 106 (explaining Congressional reaction to *Cubby* and *Stratton* decisions). "In particular, members of Congress and online intermediaries alike fretted over this nonsensical 'rule' that would result in one of two extremes." *Id.* After much debate, Congress passed the Family Empowerment Amendment ("FEA"), which provided a hands-off approach to internet regulation with limited federal intervention. *Id.* at 107. The "Good Samaritan provision" of the FEA—now known as § 230 of the CDA— allowed ISP's to self regulate. *Id*. The FEA laid the foundation of § 230. *Id.* at 108.

[26] *See* Nina I. Brown, *Fight Terror, Not Twitter: Insulating Social Media from Material Support Claims*, 37 LOY. L.A. ENT. L. REV. 1, 39 (2017) (articulating reason behind original enactment of CDA).

[27] *See id.* at 39 (providing reason for amending CDA). "[S]ection 230 was tacked on to address the growing concern that websites could be liable for content posted by third parties." *Id.* One year after the CDA was enacted, most of the Act was struck down as unconstitutional; however, § 230 was kept in tact. *Id.*

[28] *See* 47 U.S.C. § 230(c)(1) (2019) (providing immunity to internet providers for third-party content posts on their sites); *see also* Brown, *supra* note 26, at 37 ("Simply put, section 230 protects social media sites, among others, from civil liability for publishing content such as posts, pages, comments, tweets, etcetera generated by its users."); Jeff Magenau, *Setting Rules in Cyberspace: Congress's Lost Opportunities to Avoid the Vagueness and Overbreadth of the Communications Decency Act*, 34 SAN DIEGO L. REV. 1111, 1112 (1997) (discussing enactment of CDA).

[29] *See* Brown, *supra* note 26, at 39 (citing legislative purpose of § 230). Congress' main purpose and goal at the time of enacting the CDA was to encourage the development and free flow of information through the internet. *Id.* Furthermore, "[i]n passing section 230 and allowing sites to voluntarily filter content, Congress spared social media platforms from the grim choice of either performing some content-editing to remove obscene and offensive material or policing no content at all." *Id.* at 41.

under § 230 of the CDA: "(1) the defendant must be a provider or user of an 'interactive computer service'; (2) the asserted claims must treat the defendant as a publisher or speaker of information; and (3) the challenged communication must be 'information provided by another information content provider.'"[30]

In *Zeran v. America Online, Inc.*, the United States Court of Appeals for the Fourth Circuit became the first court to interpret the CDA and subsequently set the precedent of broad immunity for internet service providers.[31] The court stated that "lawsuits 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."[32] With the exception of the Ninth Circuit, most courts have followed the *Zeran* precedent, holding that § 230 provides broad immunity to internet providers in the interest of cultivating a dynamic and open-internet system.[33] In *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, the Ninth Circuit limited § 230 and held that an ISP should not be afforded immunity because "it created and designed its registration process around questions and answers that it provided to prospective subscribers, which made Roommates.com analogous to an information

---

[30] *See id.* at 43 (laying out three elements that must be satisfied for § 230 immunity).

[31] *See* 129 F.3d 327, 330 (4th Cir. 1997) (explaining application of § 230 and immunity it provides for ISPs); *see also* Jee, *supra* note 21, at 187 ("Ultimately, *Zeran v. America Online*, *Inc*. greatly expanded the scope of immunity afforded by the CDA, concluding that the distinction between 'distributor' and 'publisher' was irrelevant.")

[32] *See Zeran*, 129 F.3d at 330 (discussing legislative history and intent of § 230). "In specific statutory findings, Congress recognized the Internet and interactive computer services as offering 'a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.'" *Id.* (citations omitted).

[33] *See* Doe v. Backpage.com, LLC, 817 F.3d 12, 29 (1st Cir. 2016) (following precedent and holding internet provider not liable under CDA). *Doe* involved an internet service provider aiding in the solicitation of sex trafficking of minors. *Id.* at 16. The court stated that these circumstances "evoke outrage." *Id.* at 15. However, the court also stated that unfortunately, "Congress did not sound an uncertain trumpet when it enacted the CDA, and it chose to grant broad protections to internet publishers. Showing that a website operates through a meretricious business model is not enough to strip away those protections." *Id.* at 29. *Doe* is an example of how courts reluctantly feel bound to interpret immunity of the CDA broadly. *Id.* at 19; s*ee also* Phe, *supra* note 2, at 112 (explaining impact of *Zeran* decision). "Because *Zeran* was the first major case to interpret § 230, the Fourth Circuit's decision to eliminate notice-based liability and grant broad immunity to ISPs had far-reaching consequences: it set the tone for the judicial development and construction of § 230." Phe, *supra* note 2, at 112. *But see* FTC. v. LeadClick Media, LLC, 838 F.3d 158, 176 (2d Cir. 2016) (holding "LeadClick is an information content provider with respect to the deceptive content at issue and is not entitled to immunity under Section 230."); Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1109 (9th Cir. 2009) (finding Yahoo! not immune for matchmaking algorithms); Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir. 2003) (suggesting § 230 should be read "as a definitional clause rather than as an immunity from liability, and thus harmonize the text with the caption.").

content provider."[34] The Seventh Circuit also provided language against a broad application of the CDA, but ultimately gave immunity to the ISP.[35]

In *Force*, the court started its analysis by emphasizing the precedent courts' findings that § 230 provides broad immunity.[36] The court then implemented an ordinary meaning of the word "publisher" and categorized Facebook as such.[37] The court rejected the Plaintiffs' argument that Facebook should be liable for providing Hamas a platform to organize and reasoned that Facebook's conduct "falls within the heartland of what it means to be the 'publisher' of information under Section 230(c)(1)."[38] Furthermore, Facebook's use of algorithms and "matchmaking" tools to connect Hamas supporters did not disqualify Facebook from being considered a publisher.[39] The court stated that the bulk of an interactive computer service's job is to decide what content to display and noted there is no precedent that denied § 230 immunity based on "matchmaking."[40]

---

[34] *See* 521 F.3d 1157,1175 (9th Cir. 2008) (rejecting immunity for internet service provider); *see also* Phe, *supra* note 2, at 114 (noting importance of Roommates.com as only case to limit CDA immunity). This case was one of a "few instances where a court narrowed its interpretation of § 230 and held that immunity should not extend to the ISP in question." Phe, *supra* note 2, at 114; *see also* Madeline Byrd & Katherine J. Strandburg, *CDA 230 for a Smart Internet*, 88 FORDHAM L. REV. 405, 406 (2019) (highlighting development of internet and need to adapt CDA in line with internet-expanded capabilities); Joseph Monaghan, Comment, *Social Networking Websites' Liability for User Illegality*, 21 SETON HALL J. SPORTS & ENT. L. 499, 506 (2011) (highlighting one example of broad immunity of CDA); Andrew Bolson, *The Internet Has Grown Up, Why Hasn't the Law? Reexamining Section 230 of the Communications Decency Act*, INT'L ASS'N OF PRIVACY PROFESSIONALS (Aug. 27, 2013), https://iapp.org/news/a/the-internet-has-grown-up-why-hasnt-the-law-reexamining-section-230-of-the/ (stating effect of technological advances on application of CDA).

[35] *See Doe*, 347 F.3d at 660 ("Why should a law designed to eliminate ISPs' liability to the creators of offensive material end up defeating claims by the victims of tortious or criminal conduct?") "If this reading is sound, then § 230(c) as a whole makes ISPs indifferent to the content of information they host or transmit: whether they do . . . or do not . . . take precautions, there is no liability under either state or federal law." *Id.*

[36] *See* Force v. Facebook, Inc., 934 F.3d 53,64 (2d Cir. 2019) (laying out precedent cases' treatment of §230 immunity for internet-content providers). "In light of Congress's objectives, the Circuits are in general agreement that the text of Section 230(c)(1) should be construed broadly in favor of immunity." *Id.* at 64; *see also* Jee, *supra* note 21, at 191 (highlighting importance of deciding CDA cases based on statutory interpretation).

[37] *See Force*, 934 F.3d at 65 (explaining meaning and court's interpretation of word "publisher"). The broad interpretation of §230 immunity "has resulted in a capacious conception of what it means to treat a website operator as the publisher . . . of information provided by a third party." *Id.* (citing *Backpage.com*, 817 F.3d at 19).

[38] *See id.* at 65 (rejecting Plaintiffs' argument that Facebook is not publisher).

[39] *See id.* at 66 (finding "matchmaking" algorithms do not render internet content provider publisher). "Indeed, arranging and distributing third-party information inherently forms 'connections' and 'matches' among speakers, content, and viewers of content . . . [t]hat is an essential result of publishing. Accepting plaintiffs' argument would eviscerate Section 230(c)(1) . . . ." *Id.*

[40] *See id.* at 67 ("All of these decisions, like the decision to host third-party content in the first place, result in 'connections' or 'matches' of information and individuals, which would have

Next, the court addressed whether Facebook was a developer or creator because, if Facebook fell within either category, it would not have immunity under § 230.[41] The court rejected the Plaintiffs' argument that Facebook developed Hamas's content by directing the content to people interested in it.[42] The court reasoned that Facebook is not responsible for nor does it edit the content Hamas provides.[43] According to the court, Facebook is classified as a neutral party because the social media platform merely takes objective information from its users to "match" them with other users.[44] Facebook's act of making content more visible or available to users is part of the traditional role of a publisher and is not considered "developing" for the purposes of § 230.[45] In this instance, the court joined the majority of circuits in its broad interpretation of both § 230 of the CDA and the meaning of the word "publisher."[46]

Whether an internet provider is immune from liability for allegedly aiding a terrorist organization depends solely on the interperative mechanisms of the CDA.[47] However, courts have struggled to interpret the CDA due to the statute's lack of clearly defined terms.[48] Most circuit courts ap-

---

not occurred but for the internet services' particular editorial choices regarding the display of third-party content.")

[41] *See id.* at 68 (transitioning to Plaintiffs' argument that Facebook is developer of Hamas's content). "[C]onsistent with broadly construing 'publisher' under Section 230(c)(1), we have recognized that a defendant will not be considered to have developed third-party content unless the defendant directly and 'materially' contributed to what made the content itself 'unlawful.'" *Id.* (citing FTC. v. LeadClick Media, LLC, 838 F.3d 158, 174 (2d Cir. 2016).

[42] *See Force*, 934 F.3d at 70 (holding Facebook is not developer of content). Since Facebook users own their content, they control what they write on their pages and who can see it. *Id.* Therefore, Facebook is not a developer for purposes of § 230. *Id.*

[43] *See id.* (noting Facebook also does not "suggest edits for the content its users—including Hamas—publish").

[44] *See id.* (explaining how Facebook algorithms function). "The algorithms take the information provided by Facebook users and 'match' it to other users—again, materially unaltered—based on objective factors applicable to any content, whether it concerns soccer, Picasso, or plumbers." *Id.* Facebook's act of arranging users' objective information does not render it a developer. *Id.*

[45] *See id.* at 70 (refuting Plaintiffs' argument). "But making information more available is, again, an essential part of traditional publishing; it does not amount to "developing" that information within the meaning of Section 230." *Id.*

[46] *See id.* at 68-69 (holding Facebook immune under CDA's broad application).

[47] *See* Jee, *supra* note 21, at 191 (discussing how courts determine liability under CDA). "To analyze the CDA's meaning of 'develop,' an analysis using the canons of statutory interpretation is appropriate." *Id.*

[48] *See* Magenau, *supra* note 28, at 1113 (explaining difficulties of interpreting CDA). "However, the CDA is also problematic on a more fundamental level: it is filled with ambiguities and inconsistencies of language." *Id.* at 1113; *see also* Byrd, *supra* note 34, at 408 (articulating ambiguities in CDA language). "Because CDA 230 does not define 'publisher,' its interpretation has been a central, and difficult, task for the courts." Byrd, *supra* note 34, at 408. Furthermore, it has been suggested that the CDA:

plied a broad interpretation of the CDA, and the Second Ciruit in *Force* was not an exception to this majority rule.[49] The strength of the CDA's immunity shield is highlighted in *Doe v. Backpage.com*, where the court did not morally agree with providing immunity to the defendant, but felt that the CDA required them to do so.[50] Therefore, the *Force* decision will perpetuate broad immunity under the CDA for internet providers, making it difficult for future plaintiffs to successfully sue on these grounds.[51]

Future practicioners seeking to hold internet providers liable for their actions with third-parties may find it helpful to focus on categorizing internet providers as developers.[52] If an internet provider is classified as a

---

> [S]hould be amended to clarify that a party is not 'treated as the publisher or speaker of any information provided by another information content provider' unless liability is premised primarily on the actionable nature of that third-party content. This change preserves the sort of immunity from publisher liability that the drafters of CDA 230 had in mind.

Byrd, *supra* note 34, at 436; *see also* Brown, *supra* note 26, at 4 (noting confusion in applying § 230).

> The application of section 230 is unclear where liability is based not on the content posted by the third-party, but instead on the consequences of allowing that third party to use the social media platform. This is a critical distinction and presents a second unsettled question for courts confronting these cases.

Brown, *supra* note 26, at 4.

[49] *See* sources cited & accompanying text *supra* note 36; *see also Force*, 934 F.3d at 68 (holding Facebook immune under CDA's broad application); Monaghan, *supra* note 34, at 507 ("As a result of judicially extended immunity to ICPs, these social networking websites have also been consistently granted broad section 230 immunity.") Social media platforms have no incentive to protect their users "because of the broad immunity granted to them by judicial interpretation of section 230 of the Communications Decency Act (CDA)." Monaghan, *supra* note 34, at 500.

[50] *See* Doe v. Backpage.com, LLC, 817 F.3d 12, 15 (1st Cir. 2016) (articulating court's concerns of current CDA interpretation). "This is a hard case — hard not in the sense that the legal issues defy resolution, but hard in the sense that the law requires that we, like the court below, deny relief to plaintiffs whose circumstances evoke outrage." *Id.* at 15; *see also* Monaghan, *supra* note 34, at 506 (using *Backpage.com* to emphasize broad application of CDA).

[51] *See generally Force*, 934 F.3d at 64 (stating current trend in courts to interpret §230 broadly). "In light of Congress's objectives, the Circuits are in general agreement that the text of Section 230(c)(1) should be construed broadly in favor of immunity." *Id.* at 64; *see also* Neuburger, *supra* note 5 (noting significance of *Force* decision).

[52] *See Force*, 934 F.3d at 81(Katzmann, C.J., dissenting in part) (explaining how case precedent does not provide developers CDA immunity). Section 230 "does not necessarily immunize defendants from claims based on promoting content or selling advertising, even if those activities might be common among publishing companies nowadays." *Id.* at 81; *see also* Monaghan, *supra* note 34, at 503 (explaining difference between publishers and distributors). "The issue is substantial because under the law of most states, a publisher is strictly liable for defamatory statements, whereas a distributor is liable only for content it knew or should have known was defamatory." Monaghan, *supra* note 34, at 503.

content developer, they fall outside of the CDA immunity shield because they are no longer simply a publisher.[53] For example, Facebook's algorithmic capability to matchmake and create networks of users arguably goes far beyond a traditional publisher's ability.[54] Through these algorithms, Facebook is not merely placing an ad on the front page of a newspaper.[55] Rather, Facebook connects people in a way that generates new groups, followers, and the ability to reach people that would otherwise not be possible without those algorithms.[56] If plaintiffs can show how the internet has expanded its capabilities since the enactment of the CDA, they may be able to prove that these internet providers are more than simply publishers of their content.[57]

Furthermore, in *Force*, the court stated that holding Facebook liable for its use of algorithms would "turn Section 230(c)(1) upside down."[58]

---

[53] *See Force*, 934 F. 3d at 68 (stating that "[i]f Facebook was a creator or developer, even 'in part,' of the terrorism-related content upon which plaintiffs' claims rely, then Facebook is an 'information content provider' of that content and is not protected by Section 230(c)(1) immunity.")

[54] *See id.* at 83 (Katzmann, C.J., dissenting in part) (quoting Facebook CEO's description of Facebook). "CEO Mark Zuckerberg has similarly described Facebook as 'build[ing] tools to help people connect with the people they want,' thereby 'extending people's capacity to build and maintain relationships.'" *Id.* (citations omitted). These actions of creating social networks go beyond the traditional editorial actions the CDA immunizes. *Id.*; *see also* Jee, *supra* note 21, at 191 (citing broad interpretation of term "developer"). The meaning of developer "encompasses a broad meaning, extending beyond mirroring the definition of creation which is to '[m]ake something new' or '[c]ome into existence.' Rather, the definition of 'develop' in the CDA, as construed by the courts, is 'to make actually available or usable (something previously only potentially available or usable).'" Jee, *supra* note 21, at 191 (citing FTC v. Accusearch, Inc., 570 F.3d 1187, 1189 (10th Cir. 2011)).

[55] *See Force*, 934 F. 3d at 83 (Katzmann, C.J., dissenting in part) (explaining Facebook's increased ability to connect users); s*ee also* Bolson, *supra* note 34 (noting possible options to amend CDA to keep up with evolving technology).

[56] *See Force*, 934 F. 3d at 83 (Katzmann, C.J., dissenting in part) (explaining how algorithms "forge real-world (if digital) connections through friend and ground suggestions").

[57] *See* Monaghan, *supra* note 34, at 505 (noting development of internet since CDA was enacted).

> Notably, however, the Internet model at the time Congress enacted the CDA was very different than what has since evolved . . . [i]t is uncertain whether Congress would have afforded the same protection at the time it enacted the CDA had it known that ISPs would deliver content in the future.

Monaghan, *supra* note 34, at 505; *see also* Phe*, supra* note 2, at 101-02 (explaining how unforeseen technological advances complicate statutory interpretation). "Nevertheless, in light of today's technological advances, the legislative objectives that § 230 once served are at risk of becoming obsolete. The changing nature of the Internet demands action, and Congress has failed in this regard." Phe*, supra* note 2, at 101-02. When the CDA was enacted, the internet was a relatively new phenomenon. Phe*, supra* note 2, at 101-02.

[58] *See Force*, 934 F.3d at 67 (stating Facebook's use of algorithms does not exclude platform from being publisher).

This argument shows just how far courts have gone in applying CDA immunity to internet providers and highlighting the need for a shift in how courts interpret and apply the CDA.[59] The CDA was enacted in 1996 when the internet had far fewer capabilities than it does today.[60] Therefore, courts should not look to the CDA as a broad immunity shield, but should instead focus on the internet providers' actual actions.[61] By shifting the focus away from sweeping CDA immunity and instead focusing on the collective effect of Facebook and other social media platforms' actions with third-parties, internet providers may be held more accountable for their specific conduct.[62] A narrower interpretation of the CDA will keep with the legislative intent of the CDA, which was to protect the role of a traditional publisher, and did not account for the algorithmic capabilities of the

---

[59] *See* Phe, *supra* note 2, at 124 (explaining how terrorist organizations rely on social media platforms). The broad application of the CDA "neither incentivizes nor motivates [internet service providers] to implement measures that could have a negative impact on traffic and revenue. Victims of harmful or offensive content are often left without legal recourse because § 230 imposes a veritable challenge." *Id.* at 125; *see also* Jee, *supra* note 21, at 187 (showing sweeping effect *Zeran* decision had on immunity). The *Zeran* court feared that holding internet providers liable for "potentially tortious material would increase the costs of operation such that internet service providers would no longer seek to do business. This drastic hypothetical would run contrary to the policies the CDA was enacted to promote." Jee, *supra* note 21, at 187.

[60] *See* Monaghan, *supra* note 34, at 532 ("In the last ten years, however, technology has progressed, and social networking websites now have the means, but not the will to implement effective change."); *see also* Brown, *supra* note 26, at 7 ("About 90 percent of organized terrorism on the internet is being carried out through social media.") (citations omitted).

[61] *See Force*, 934 F.3d at 81 (Katzmann, C.J., dissenting in part) ("Section 230(c)(1) limits liability based on the function the defendant performs, not its identity."). Furthermore, "[l]ooking beyond Facebook's 'broad statements of immunity' and relying 'rather on a careful exegesis of the statutory language,' . . . the CDA does not protect Facebook's friend- and content-suggestion algorithms." *Id.* at 82 (citing Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1100 (9th Cir. 2009)); *see also* Jee, *supra* note 21, at 180 (suggesting narrower approach to applying CDA to current internet platforms). The broad application of the CDA in light of the development of technology "does not necessarily align with the objectives the Zeran court sought to achieve with its broad interpretation." Jee, *supra* note 21, at 180. Therefore, a more "fact-specific inquiry considering such factors as the type of claim being brought, the specifics of the posted content, what the internet service provider or website sought to achieve with the content, and the like, more effectively balance the policy goals of promoting internet usage with deterring illegal behavior." Jee, *supra* note 21, at 180.

[62] *See* Jee, *supra* note 21, at 196 (noting importance of considering internet-platform-specific actions when deciding liability).

> By adopting a totality of the circumstances approach to CDA immunity, social networking sites would not receive such a strong grant of immunity. Instead, a court could apply the following factors to determine whether a social networking site should be afforded immunity: 1) the type of claim being brought; 2) the specifics of the posted content; 3) any actions the internet service provider or website has taken; and, 4) the policy objectives of the CDA.

Id.

internet today.[63] Perhaps a narrow interpretation of the CDA does not go far enough; instead, an update to § 230 of the CDA would be more effective in keeping up with the rise in technology and social media platforms' abilities.[64]

The Second Circuit is one of many circuit courts faced with the issue of how to apply the CDA to social media platforms. Specifically, the court considered whether Facebook was immune from liability for allegedly aiding a terrorist organization in carrying out attacks. The Second Circuit joined a majority of courts in applying a broad interpretation of the CDA, and ultimately found Facebook immune from liability. However, this application is not reflective of the original intent of the CDA, as the internet has more capabilities today to connect people and groups. By implementing these advanced capabilities, most social media platforms have transcended the role of traditional publishers and therefore should not be provided CDA immunity.

Alison Eleey

---

[63] *See* Byrd, *supra* note 34, at 407 (laying out CDA's history and purpose). Congress enacted the CDA in response to a case that attempted to hold online bulletin boards liable for defamatory statements published on its site. *Id.* Therefore, Congress did not enact the CDA with the current algorithmic capabilities of internet providers today. *Id.* Instead, Congress felt that "[t]raditional publisher-style screening for actionable content would have been untenable for online services that provided forums for user-driven exchanges involving large amounts of rapidly changing content." *Id.*; *see also* Jee, *supra* note 21, at 180 (asserting broad interpretation of CDA immunity where social media websites fail to satisfy statutory intent). "Therefore, extending the grant of Communications Decency Act immunity to these new forms of technology does not necessarily align with the objectives the Zeran court sought to achieve with its broad interpretation." Jee, *supra* note 21, at 180.

[64] *See* Jee, *supra* note 21, at 180 (calling for revision of CDA).