Penn State Law Review

Volume 125 | Issue 2 Article 4

1-1-2021

Section 230 of the Communications Decency Act, Product Liability, and a Proposal for Preventing Dating-App Harassment

Kira Geary

Comments:

Section 230 of the Communications Decency Act, Product Liability, and a Proposal for Preventing Dating-App Harassment

Kira M. Geary*

ABSTRACT

For ten months, Matthew Herrick endured a continuous campaign of harassment that was remotely coordinated by his ex-boyfriend. Herrick's ex used the dating app Grindr to send over 1,400 men to harass Herrick, both at Herrick's home and place of work. Herrick sent over 100 complaints to Grindr, several cease-and-desist letters, and even obtained a temporary injunction ordering Grindr to ban his ex from using its services. However, despite Herrick's efforts, Grindr refused to take any action. Herrick then filed suit, bringing product liability claims against Grindr for failing to implement widely used safety features in its software to protect its consumers from injury. Nonetheless, both the Southern District of New York and the Second Circuit Court of Appeals found that Grindr was immune from liability under Section 230 of the Communications Decency Act.

* J.D. Candidate, The Pennsylvania State University, Penn State Law, 2021.

Herrick v. Grindr fits within a line of cases in which courts have interpreted Section 230's scope so broadly that interactive computer services ("ICSs") now enjoy near-total civil immunity. This broad immunity has come at the cost of consumer safety, and plaintiffs like Herrick, who allege injuries due to defectively designed or defectively manufactured app software, have been left largely without a legal remedy.

This Comment uses the flawed reasoning in the *Herrick v. Grindr* line of decisions to explain why Section 230 should not shield ICSs from liability when they fail to enact widely available safeguards to protect their apps' consumers from abuse and violence. This Comment explains why product liability claims like Herrick's should be permitted as a remedy for injuries resulting from poorly designed or poorly manufactured software that fails to protect users from foreseeable harm. Ultimately, this Comment argues that Congress, using the Fight Online Sex Trafficking Act ("FOSTA") as a framework, should amend Section 230 to allow product liability suits to be brought against ICSs.

Table of Contents

I. INTRODUCTION

Matthew Herrick became the victim of a ten-month-long harassment campaign after his ex-boyfriend used the dating app Grindr[1] to send over 1,400 strangers to Herrick's home and place of work.[2] Each of the men sent to visit Herrick expected sex; Herrick's ex even instructed some men to interpret Herrick's resistance as "part of an agreed upon rape fantasy."[3] Herrick's ex created fake Grindr profiles that impersonated Herrick and even managed to manipulate Grindr's geolocation tools[4] to make it seem as if the messages were coming from Herrick's location, including Herrick's home and place of work.[5] Herrick repeatedly sought Grindr's help in ending the harassment campaign.[6] However, after more than 100 complaints, a cease-and-desist letter, and a temporary court injunction, Grindr refused to take any action.[7]

In 2017, Herrick filed suit against Grindr, alleging defects in design, manufacture, and warning, among other claims.[8] Herrick's product liability claims[9] alleged that Grindr's app was a defective product because its software was easily exploited and lacked the ability to identify and exclude abusive users when safeguards to prevent this

---

1. Grindr is "the world's largest social networking app for gay, bi, trans, and queer people." *About*, GRINDR, https://www.grindr.com/about/ (last visited Aug. 28, 2020). Grindr reported that, in 2013, more than one million users logged in to the app every day and sent more than seven million messages and two million photos. *See* Ari Ezra Waldman, *Law, Privacy, and Online Dating: "Revenge Porn" in Gay Online Communities*, 44 L. & SOCIAL INQUIRY 987, 990 (2019).

2. *See* Carrie Goldberg, *Herrick v. Grindr: Why Section 230 of the Communications Decency Act Must Be Fixed*, LAWFARE (Aug. 14, 2019, 8:00 AM), http://bit.ly/2vsB3Xf. The author of this piece, Carrie Goldberg, was one of Herrick's attorneys. *See* First Amended Complaint at *42, Herrick v. Grindr, LLC, 306 F. Supp. 579 (S.D.N.Y. 2019) (No. 17-CV-932 (VEC)).

3. Andrew Schwartz, *The Grindr Lawsuit That Could Change the Internet*, OUTLINE (Jan. 11, 2019, 2:02 PM), http://bit.ly/2NrnEFw.

4. "Geolocation is a technology that uses data acquired from an individual's computer or mobile device to identify or describe the user's actual physical location." Betsie Estes, *Geolocation—The Risk and Benefits of a Trending Technology*, INFO. SYS. AUDIT & CONTROL ASS'N (Sept. 26, 2016), http://bit.ly/388dP6R.

5. *See* Goldberg, *supra* note 2.

6. *See id.*

7. *See* Schwartz, *supra* note 3.

8. Other claims Herrick brought against Grindr include: negligence, copyright infringement, promissory estoppel, fraud, violations of New York's Deceptive Business Practices Act, violations of New York's False Advertising Law, intentional infliction of emotional distress, negligent infliction of emotional distress, and negligent misrepresentation. *See* First Amended Complaint, *supra* note 2, ¶¶ 100–216.

9. Product liability is "[a] manufacturer's or seller's tort liability for any damages or injuries suffered by a buyer, user, or bystander as a result of a defective product." *Products Liability*, BLACK'S LAW DICTIONARY (11th ed. 2019); *see also infra* Section II.C (explaining traditional product liability causes of action). Herrick's product liability claims included defect in design, defect in manufacture, and defect in warning. *See* First Amended Complaint, *supra* note 2, ¶ 13.

danger were available for Grindr to implement.[10] Herrick also alleged that Grindr failed to warn users that its app could be "weaponized and used to impersonate and abuse," and that a warning that alerts app users of the potential for abuse would have prevented Herrick from downloading the app, thereby preventing his injuries.[11]

Both the United States District Court for the Southern District of New York and the Second Circuit Court of Appeals, however, held that Section 230 of the Communications Decency Act ("CDA")[12] barred Herrick's claims before his allegations about Grindr's faulty geolocation technology could be examined.[13] The Southern District of New York reasoned that "Herrick's design and manufacturing defect, negligent design, and failure to warn claims are all based on content provided by another user—Herrick's former boyfriend."[14] According to the court, the fact that Herrick's ex-boyfriend put content onto Grindr gave Grindr immunity under Section 230, because an interactive computer service ("ICS")[15] cannot be held liable for content if it did not contribute to the development of what made the content unlawful.[16] Despite Herrick having no opportunity to show how Grindr's geolocation technology was defective, the court determined that the geolocation tools were for "neutral assistance"[17] and were thus permissible under Section 230.[18] In October 2019, the Supreme Court denied certiorari in Herrick's case.[19]

This Comment argues that, by broadening the scope of Section 230 to preclude product liability suits against ICSs simply because an injury involved some kind of third-party content, the courts deciding *Herrick* allow ICSs to put defectively designed software into the stream of commerce without fear of liability.[20] In Part II, this Comment first

10. *See* First Amended Complaint, *supra* note 2, ¶¶ 100–15, 121–26.

11. *Id.* ¶¶ 117, 129.

12. *See* 47 U.S.C. § 230 (2018).

13. *See* First Amended Complaint, *supra* note 2, ¶¶ 101, 104, 109, 112, 117, 122; *see also* Herrick v. Grindr, LLC, 306 F. Supp.3d 579, 588 (S.D.N.Y. 2018), *aff'd*, 765 Fed. Appx. 586 (2d Cir. 2019).

14. *Herrick*, 306 F. Supp. at 589.

15. An interactive computer service ("ICS") is "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. § 230(f)(2); *see also infra* Section II.B.

16. *See Herrick*, 306 F. Supp. at 589.

17. ICSs are permitted to create "neutral tools" that may facilitate illicit or unlawful conduct without being considered a developer of the content, so long as that tool does not contribute to the content's illegality. *See* Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1169 (9th Cir. 2008); *see also infra* Section II.B.

18. *See Herrick*, 306 F. Supp. at 590.

19. Alexis Kramer, *Grindr Harassment Case Won't Get Supreme Court Review*, BLOOMBERG LAW (Oct. 7, 2019, 9:51 AM), http://bit.ly/2wcC3Q1.

20. *See infra* Part III.

addresses the advent of the Communications Decency Act ("CDA"), with particular emphasis on the broadening application of Section 230 of the CDA.[21] Part II also addresses the fundamental principles of product liability claims in tort.[22] In Part III, this Comment argues that courts have expanded Section 230 to cover nearly every type of civil claim against ICSs, which not only runs contrary to much of Section 230's underlying rationale, but is also antithetical to modern principles of consumer protection.[23] Part III also applies the principles of traditional product liability to situations where an injury was allegedly caused by a defect in the design or manufacture of an app's software.[24] Part III ultimately argues that Congress should amend Section 230 to allow plaintiffs to bring product liability suits against app developers when their injuries were caused by defectively designed or defectively manufactured software.[25] Finally, in Part IV, this Comment offers concluding statements on the foregoing discussion.[26]

II. BACKGROUND

When the internet became freely available to the public in the 1990s, lawmakers grew concerned about the increasing availability of indecent, obscene, and pornographic materials.[27] As the internet became a common feature of the American home, lawmakers especially sought to protect children from cyber-stalking, harassment, and open access to pornography.[28]

A. The Advent of the CDA

In response to the increasing availability of pornographic materials online, Congress initially passed the CDA to generally regulate online obscenity and indecency.[29] Legislators sought to "extend and strengthen the protections which exist against harassing, obscene, and indecent phone calls to cover all such uses of all telecommunications devices" and to protect children "from those who would electronically cruise the digital world to engage children in inappropriate communications and

21. *See infra* Section II.B.
22. *See infra* Section II.C.
23. *See infra* Section III.A.
24. *See infra* Section III.B.
25. *See infra* Section III.C.
26. *See infra* Part IV.
27. *See* Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. 51, 53 (1996).
28. *See id.*
29. *See id.*

introductions."[30] In 1997, however, the United States Supreme Court unanimously held that the anti-indecency restrictions contained in the CDA violated the First Amendment.[31]

Section 230 of the CDA, however, survived the Supreme Court's scrutiny.[32] Legislators passed Section 230 of the CDA in response to two court cases concerning ICS liability for defamation claims, which had divergent outcomes.[33] In *Cubby Inc. v. CompuServe, Inc.*,[34] the United States District Court for the Southern District of New York held that an ICS could not be held liable for defamation that took place on the ICS's site because the ICS did not review any of the content posted on the forums.[35] By contrast, in *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[36] the Supreme Court of Nassau County, New York held that an ICS was liable for the content of all the posts on its site because it routinely moderated its online message boards.[37] The decisions in *Cubby* and *Stratton Oakmont* created uncertainty regarding free speech on the internet and gave legislators concern that these types of suits could stunt the vital emerging technology of electronic communication on the internet.[38] Lawmakers sought to balance the concern of stifling online speech with the desire to promote the screening and removal of obscene and offensive material, a balance supported by the underlying purpose of the CDA as a whole.[39]

The text of CDA's Section 230[40] plainly expresses Congress's intent.[41] Section 230 states that Congress's goal was:

---

30. 141 Cong. Rec. S1944-01 (Feb. 1, 1995) (statement of Sen. J. James Exon). *See generally* 141 Cong. Rec. S8087-04 (June 9, 1995) (statement of Sen. J. James Exon) ("The heart and the soul of the Communications Decency Act [is] its protection for families and children.").

31. *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844, 849 (1997).

32. *See CDA 230: Legislative History*, ELEC. FRONTIER FOUND., https://bit.ly/3pfWD8Y (last visited Feb. 11, 2020).

33. *See* Leslie Paul Machado, *Immunity Under § 230 of the Communications Decency Act of 1996: A Short Primer*, 10 No. 3 J. INTERNET L. 3 (2006); *see also supra* note 15 and accompanying text.

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

35. *See id.* at 142.

36. Stratton Oakmont, Inc. v. Prodigy Servs. Co., INDEX No. 31063/94, 1995 WL 323710 (Sup. Ct. Nassau Cty. May 24, 1995).

37. *See id.*

38. *See* Machado, *supra* note 33.

39. *See generally* 141 Cong. Rec. H8460-1 (daily ed. Aug. 4, 1995) (statement of Rep. Christopher Cox) (explaining that Section 230 would "protect computer Good Samaritans, online service providers, anyone who provides a front end to the Internet, let us say, who takes steps to screen indecency and offensive material for their customers . . . from taking on liability such as occurred in the *Prodigy* case in New York that they should not face for helping us and for helping us solve this problem").

40. Prior to its enactment, Section 230 was originally referred to as the "Online Family Empowerment Amendment," or the Cox-Wyden Amendment. *See id.*

> (1) [T]o promote the continued development of the Internet and other interactive computer services and other interactive media; (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation; (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services; (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and (5) to *ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer*.[42]

Section 230, entitled "Protection for 'Good Samaritan' blocking and screening of offensive material" provides: "No provider or user of an interactive computer service ["ICS"] shall be treated as the publisher or speaker of any information provided by another information content provider ["ICP"]."[43] While most courts today use Section 230 to protect ICSs from liability for under-screening, Section 230's text addresses *both* under-screening and over-screening done in good faith:

> [N]o provider or user of an interactive computer service ["ICS"] shall be held liable on any action voluntarily taken in good faith to restrict access to 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.[44]

Courts have since interpreted Section 230's text to bar a vast array of claims against ICSs, effectively expanding Section 230's scope.[45]

---

41. *See generally* 47 U.S.C. § 230(a)–(b) (2018) (explaining Congress's intent in passing Section 230).

42. *Id.* § 230(b) (emphasis added).

43. *Id.* § 230(c)(1). An information content provider ("ICP") is "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other [ICS]." *Id.* § 230(f)(3). However, where an ICS and an ICP are the same party, Section 230 does not provide immunity. *See* Sean Flaherty & Gordon Rees Scully Mansukhani LLP, *Section 230 Remains a Powerful Weapon to Defend Online Businesses*, LEXOLOGY (Oct. 28, 2016), http://bit.ly/2JnMbc8.

44. 47 U.S.C. § 230(c)(2).

45. *See generally* Danielle Keats Citron & Benjamin Wittes, *The Problem Isn't Just Backpage: Revising Section 230 Immunity*, 2 GEO. L. TECH. REV. 453, 458 (2018) (explaining that "federal courts have reached a near-universal agreement that [Section 230] should be construed broadly"); *see also* Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, No. 19-1284, 2020 U.S. LEXIS 4834 (Oct. 13, 2020) (Thomas, J.) ("[M]any courts have construed the law broadly to confer sweeping immunity on some of the largest companies in the world.").

B. Section 230's Broadening Application

Since Section 230's passage, courts have interpreted the provision's protections for ICSs to have a sweeping scope beyond simply protecting "Good Samaritan" blocking, as the statutory language provides.[46] While the Supreme Court has declined to weigh in on Section 230's scope,[47] most lower federal courts have focused on Congress's intent of "promoting unfettered speech on the Internet" while neglecting to consider the provision's other purpose—incentivizing ICSs to block and screen offensive or obscene material through providing them immunity for such filtering.[48] Indeed, most courts have ignored lawmakers' wishes of promoting ICSs' ability to block or filter offensive material and have interpreted Section 230 to "establish broad federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."[49] Some circuits, however, have interpreted Section 230 more narrowly, stating that the statute does not provide a "general immunity from liability deriving from third-party content."[50] These courts usually apply a three-tiered test to any cases in which an ICS claims Section 230 immunity.[51]

However, Section 230's legislative intent does not clearly define what constitutes an ICS under the statute, so reviewing courts have been left to determine what is considered an ICS on their own.[52] Emphasizing one part of Section 230's underlying policy rationale,[53] courts have interpreted Section 230's definition of an ICS broadly, and consider

---

46. *See* generally Citron & Wittes, *supra* note 45 (explaining that courts have expanded Section 230's original scope to reach beyond Congress's original intent).

47. *See id.* at 458.

48. *See id.* at 458–59.

49. Jones v. Dirty World Entm't Recordings, LLC, 755 F.3d 398, 407 (6th Cir. 2014) (quoting Almeida v. Amazon.com, Inc., 456 F.3d 1316, 1321 (11th Cir. 2006)); *accord* Johnson v. Arden, 614 F.3d 785, 791 (8th Cir. 2010); Doe v. Myspace, Inc., 528 F.3d 413, 418 (5th Cir. 2008); Chi. Lawyers Comm. For Civ. Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 671 (7th Cir. 2008); Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 418–19 (1st Cir. 2007); Batzel v. Smith, 333 F.3d 1018, 1026–30 (9th Cir. 2003); Green v. Am. Online (AOL), 318 F.3d 465, 471 (3d Cir. 2003); Ben Ezra, Weinstein & Co. v. AOL, 206 F.3d 980, 984–85 (10th Cir. 2000); Zeran v. AOL, 129 F.3d 327, 328 (4th Cir. 1997).

50. Barnes v. Yahoo! Inc., 570 F.3d 1096, 1100 (9th Cir. 2009); *accord* FTC v. LeadClick Media, LLC, 838 F.3d 158, 173–74 (2d Cir. 2016).

51. *See Barnes*, 570 F.3d at 1100–01. This three-tiered test requires the court to first examine whether the party claiming immunity is, in fact, a "provider or user" of an ICS. *See id.* Second, the court determines whether the party claiming immunity could be treated as the "publisher or speaker" of the content. *See id.* Finally, the court determines whether the content at issue is "information provided by another information content provider." *Id.*

52. *See supra* note 15 and accompanying text.

53. *See* 47 U.S.C. § 230(b)(1)–(2) (2018).

nearly any product that connects a user to the internet to be an ICS.[54] Courts have similarly taken a broad approach in analyzing what should be considered content from an "internet content provider" under Section 230.[55] Section 230's vague definition of an ICP is at the core of most courts' reading a broad immunity into Section 230.[56] The language of the statute ensures that an ICS will not be "treated" as the "publisher or speaker" of third-party content for the purposes of determining an ICS's civil liability.[57] Thus, the key question for courts becomes whether the plaintiff's cause of action requires the court to treat the ICS as if it were the "publisher or speaker" of the content at issue.[58] If courts find that an ICS is not the "publisher or speaker" of the content at issue, then Section 230 bars any civil action against that ICS concerning the content's publication or removal.[59]

Further, most courts have enforced Section 230 immunity for ICSs even if they aided in the creation of the allegedly tortious or unlawful content.[60] Specifically, some courts have held that ICS-created "neutral tools"[61] that facilitate unlawful or illicit activities are protected under Section 230.[62] The court in *Herrick*, for example, stated: "[a]n ICS is not the creator of offensive content unless it contributes to the 'development

54. *See* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003) ("[R]eviewing courts have treated § 230(c) immunity as quite robust, adopting a relatively expansive definition of 'interactive computer service'. . . . Under the statutory scheme, an 'interactive computer service' qualifies for immunity so long as it does not also function as an 'information content provider' for the portion of the statement or publication at issue."); *see also* Herrick v. Grindr, LLC, 306 F. Supp. 3d 579, 589 (S.D.N.Y. 2018), *aff'd*, 765 Fed. Appx. 586 (2d Cir. 2019) (describing an ICS as a service that "provides its subscribers with access to a common server").

55. *See Herrick*, 306 F. Supp. at 591 (finding that all causes of action sought to treat Grindr as the publisher of the impersonating profiles).

56. Section 230 defines an information content provider ("ICP") as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other [ICS]." 47 U.S.C. § 230(f)(3).

57. *Id.* § 230(c)(1); *see also* Barnes v. Yahoo! Inc., 570 F.3d 1096, 1101 (9th Cir. 2009).

58. *See, e.g.*, *Herrick*, 306 F. Supp. at 590 ("The third element of immunity under Section 230(c) is satisfied because the Amended Complaint seeks to hold Grindr liable as the 'publisher' or 'speaker' of the impersonating profiles.").

59. *See id.*

60. *See generally* Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019) (holding that Facebook did not "develop" *content* of postings on their website by terrorist organizations when it developed *algorithms* designed to utilize users' information to match them with other users).

61. "Neutral tools" are tools used by ICSs that only "passively transmit[] information provided by others," and do not materially contribute to the unlawful conduct in question. *See* Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1165 (9th Cir. 2008).

62. *See id.* at 1169 ("[P]roviding neutral tools to carry out what may be unlawful or illicit searches does not amount to 'development' for purposes of the immunity exception.").

of what [makes] the content unlawful.'"[63] In *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*,[64] however, the Ninth Circuit held that Section 230 did *not* shield an ICS whose questionnaire violated the Fair Housing Act.[65] The court distinguished between neutral tools and tools that contribute to the allegedly unlawful conduct.[66] Thus, even if an ICS facilitates the transmission of unlawful or tortious content, it will be immune from liability unless it "directly participates in developing the alleged illegality."[67]

While Section 230 has had a positive impact on preserving free speech online, it has also allowed the internet to flourish into an almost completely immune host for illegal conduct, which runs contrary to the intentions many lawmakers had in passing the provision.[68] As a result, debates have emerged over Section 230's vast scope.[69] For example, the Ninth Circuit Court of Appeals has declined to extend Section 230 to provide immunity for contract claims and some failure-to-warn claims.[70] Additionally, one review of all Section 230-related court opinions published between July 1, 2015 and June 30, 2016 found that, in approximately half of the cases, courts did not grant full Section 230

63. *Herrick*, 306 F. Supp. at 589 (quoting FTC v. LeadClick Media, LLC, 838 F.3d 158, 174 (2d Cir. 2016)); *see also Roommates.com*, 521 F.3d at 1167 ("[A] website helps to develop unlawful content, and thus falls within the exception to [S]ection 230, if it contributes materially to the alleged illegality of the conduct.").

64. *Roommates.com*, 521 F.3d at 1157.

65. *See id.* at 1175. The Fair Housing Act is codified at 42 U.S.C. §§ 3601–19 (2018).

66. *See Roommates.com*, 521 F.3d at 1165. In *Roommates.com*, the Ninth Circuit reasoned that Section 230 did not apply because Roommates.com "designed its search system so it would steer users based on the [discriminatory] preferences and personal characteristics that [Roommates.com] itself forces subscribers to disclose." *Id.* at 1166.

67. *Id.* at 1174.

68. *See* Citron & Wittes, *supra* note 45, at 472 ("An overbroad reading of the CDA has given platforms a free pass to ignore destructive activities and, worse, to solicit unlawful activities while doing what they can to ensure that abusers cannot be identified.").

69. *See, e.g.*, David Ingram & Jane C. Timm, *Why Republicans (and Even a Couple of Democrats) Want to Throw Out Tech's Favorite Law*, CNBC (Sept. 3, 2019, 8:28 AM), https://cnb.cx/3bAyYth.

70. *See* Barnes v. Yahoo! Inc., 570 F.3d 1096, 1109 (9th Cir. 2009) (holding that a breach of contract claim under the theory of promissory estoppel was not barred by Section 230 when an ICS allegedly promised the plaintiff that it would remove content but failed to do so); *see also* Doe v. Internet Brands, Inc., 824 F.3d 846, 853 (9th Cir. 2016) (holding that Section 230 did not bar a negligence failure-to-warn claim when a plaintiff was raped by predators who contacted her on a modeling website posing as recruiters after the ICS had knowledge of the predators' scheme and did not warn users of the site about this danger).

immunity.[71] Such a rate is significantly less than the frequency at which courts granted full immunity to ICSs in Section 230's early years.[72]

While Congress historically has taken steps to extend Section 230's protections into new areas of the law,[73] in recent years, lawmakers have attempted to curb the scope of Section 230 as it pertains to the use of ICSs to facilitate sex trafficking.[74] Congress passed the "The Fight Online Sex Trafficking Act" ("FOSTA") in 2018, which amended the CDA and created liability for ICSs if any third-party content on their websites "unlawfully promote[s] or facilitate[s] prostitution" and also imposes liability on "websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims."[75] FOSTA was passed in the immediate aftermath of the First Circuit Court of Appeals' holding in *Doe v. Backpage.com, LLC*,[76] which largely ignored Congress's stated intent of "ensur[ing] vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer."[77] In *Backpage.com*, the court protected an ICS that provided online advertising from liability under Section 230 when the provider posted advertisements of sex trafficking victims under the age of 18 and labeled the victims as escorts.[78]

---

71. *See* Jeff Kosseff, *The Gradual Erosion of the Law that Shaped the Internet: Section 230's Evolution over Two Decades*, 18 COLUM. SCI. & TECH. L. REV. 1, 3–4 (2016).

72. *See id.* ("In 2001 and 2002, courts issued 10 written opinions in which civil defendants claimed Section 230 immunity. Of those 10 opinions, eight opinions held that the defendant online intermediaries were immune from claims arising from third-party content. The only two cases in which a court declined to immunize an online intermediary involved trademark infringement claims, which are intellectual property claims that Section 230 explicitly exempts from immunity.").

73. *See* 28 U.S.C. § 4102(c)(1) (2018) (providing that "a domestic court shall not recognize or enforce a foreign judgment for defamation against the provider of an interactive computer service" if the judgment would be inconsistent with Section 230); *see also* 47 U.S.C. § 941(e)(1) (2018) (extending Section 230's scope to include a new domain, ".kids," which provides access to only materials suitable for minors).

74. *See* Aja Romano, *A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet as We Know It*, VOX (July 2, 2018, 1:08 PM), http://bit.ly/2Jz7uI2.

75. *See* Zeynep Kahveci, *Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA): Senate Passes Bill Making Online Platforms Liable for Third-Party Content Enabling Illegal Sex-Trafficking*, JOLT DIGEST & HARV. L. SCH. (Apr. 4, 2018), http://bit.ly/31SAxye.

76. Doe v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016).

77. 47 U.S.C. § 230 (2018); *see also Backpage.com*, 817 F.3d at 22.

78. *See Backpage.com*, 817 F.3d at 22. Congress's passage of SESTA/FOSTA immediately responded to the court's comment in *Backpage.com* that "[i]f the evils that the appellants have identified are deemed to outweigh the First Amendment values that drive the CDA, the remedy is through legislation, not through litigation." *Id.* at 40.

Additionally, in response to an alleged bias against conservative speech by Big Tech,[79] many conservative lawmakers have sought to limit ICSs' ability to curate the content that appears on their sites.[80] In May of 2020, seemingly in response to Twitter's removal of some of then-President Trump's tweets that shared false information,[81] Mr. Trump signed an executive order that seeks to "prevent[] online censorship" and denies companies Section 230 immunity "when they use their power to censor content and silence viewpoints that they dislike."[82]

Justice Clarence Thomas also recently urged the Supreme Court to define the proper scope of Section 230. Concurring in the denial of certiorari in a recent Section 230-related case, Justice Thomas asserted that "in an appropriate case, [the Court] should consider whether the text of this increasingly important statute aligns with the current state of immunity enjoyed by Internet platforms."[83] In support of his assertion, he cited to *Herrick* as an example of "[c]ourts . . . extend[ing] § 230 to protect companies from a broad array of traditional product-defect claims."[84]

These debates about free-speech infringement highlight the concern that both courts and lawmakers have regarding emerging technologies' place within the judicially-broadened scope of Section 230—technologies uncontemplated by Section 230's drafters.[85]

Anticipating that Grindr would likely use Section 230 to defend its refusal to protect Herrick from his ex-boyfriend's use of the app, Herrick sued Grindr under product liability theory.[86] Herrick's novel approach sought to employ an area of the law not traditionally associated with speech to hold Grindr accountable for its product's defects.[87]

---

79. "Big Tech refers to the major technology companies such as Apple, Google, Amazon and Facebook, which have inordinate influence." *Definition of: Big Tech*, PC MAG. (2019), https://bit.ly/3f3lmso (last visited Aug. 28, 2020).

80. *See* Ingram & Timm, *supra* note 69.

81. *See* Jess Miers, *A Primer on Section 230 and Trump's Executive Order*, BROOKINGS (June 8, 2020), https://brook.gs/3j007sl.

82. Exec. Order No. 13,925, 85 F.R. 34079 (2020).

83. Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, No. 19-1284, 2020 U.S. LEXIS 4834, at *2 (Oct. 13, 2020).

84. *Id.* at *10–11 (citing Herrick v. Grindr, LLC, 765 Fed. Appx. 586, 591 (2d Cir. 2019)) ("One court granted immunity on a design-defect claim concerning a dating application that allegedly lacked basic safety features to prevent harassment and impersonation.").

85. *See generally* Citron & Wittes, *supra* note 45 ("Section 230 immunity has enabled innovation and expression beyond the imagination of the operators of early bulletin boards and computer service providers the provision was designed to protect.").

86. *See generally* First Amended Complaint, *supra* note 2 (suing Grindr and bringing product-liability causes of action against it); *see also* Goldberg, *supra* note 2.

87. *See* Goldberg, *supra* note 2 ("I made sure not to sue Grindr for traditional publication torts like defamation. That is, I was not suing them for any words that

C. Traditional Product Liability Doctrines

Product liability is a common-law doctrine that seeks to protect consumers from injuries resulting from poorly designed or poorly manufactured products.[88] As product liability law developed, courts routinely relied on two theories of liability for defective products: an implied warranty of merchantability[89] and negligence.[90] Both theories, however, required that the plaintiff establish a contractual relationship with the manufacturer of the product.[91] Plaintiffs who were unable to establish such a relationship were unable to recover under either theory.[92]

Strict liability was judicially created, in part, because of dissatisfaction with the ability of both commercial law and negligence law to protect consumers against defective products.[93] The origins of product liability can be traced to the late-nineteenth century, when the new technology of the Industrial Revolution created "an accident crisis like none the world had ever seen and like none any Western nation has witnessed since."[94] As the "ever-increasing capacity of institutions to harm in mass quantities was becoming evident," courts acknowledged that laws should hold the manufacturers of dangerous products accountable when those manufacturers fail to provide basic protections for consumers.[95] In 1916, the New York Court of Appeals first held in *MacPherson v. Buick Motor Co.*[96] that manufacturers could be liable for placing a dangerous instrumentality into the stream of commerce when the damage caused by the instrumentality was foreseeable.[97] When a

---

Gutierrez said on the profiles or communications he'd made on the app. Instead, I tried something new—I sued Grindr using traditional product liability torts.").

88. *See generally Products Liability*, BLACK'S LAW DICTIONARY (11th ed. 2019) (defining product liability).

89. The implied warranty of merchantability is "[a] merchant seller's warranty—implied by law—that the thing sold is fit for its ordinary purposes." *Warranty*, BLACK'S LAW DICTIONARY (11th ed. 2019).

90. *See* Tiffany Colt, *The Resurrection of the Consumer Expectation Test: A Regression in American Products Liability*, 26 U. MIAMI INT'L & COMP. L. REV. 525, 528 (2019).

91. *See id.*

92. *See id.*

93. *See* Angela Rushton, *Design Defects Under the Restatement (Third) of Torts: A Reassessment of Strict Liability and the Goals of a Functional Approach*, 45 EMORY L.J. 389, 393 (1996); *see also* Greenman v. Yuba Power Prods., Inc., 377 P.2d 897, 899 (1963) (declining to apply the notice requirement of commercial law to a product liability claim, and reasoning that "as applied to personal injuries . . . [the notice requirement] becomes a booby-trap for the unwary").

94. John Fabian Witt, *Toward a New History of American Accident Law: Classical Tort Law and the Cooperative First-Party Insurance Movement*, 114 HARV. L. REV. 690, 694 (2001).

95. *Id.*

96. MacPherson v. Buick Motor Co., 111 N.E. 1050 (N.Y. 1916).

97. *See id.* at 1053.

product liability claim is brought in strict liability, a plaintiff need only show that the seller is "engaged in the business of selling such a product, and . . . [the product] is expected to and does reach the user or consumer without substantial change in the condition in which it is sold."[98]

Beginning in 1963, states began to impose strict liability on the manufacturers of defective products.[99] As strict liability developed, the Restatement (Second) of Torts explicitly removed any requirement that a consumer have a contractual relationship with a product manufacturer for the manufacturer to be held liable.[100] Courts used the Restatement (Second) to establish two tests for determining whether a product was defective: the consumer expectations test, which focuses on whether a product fails to meet the safety expectations of an ordinary consumer, and the risk-utility test, which balances the benefits of avoiding a safety risk with the costs of doing so.[101]

In 1998, the Restatement (Third) of Torts: Products Liability recognized three major types of judicially created product liability claims.[102] These categories—dangerous product design, manufacturing defect, and failure to provide adequate warning—were each given distinct liability rules.[103] In *Herrick*, the plaintiff brought claims under all three of these causes of action from the Restatement (Third).[104]

1. Defective Product Design

A product is defective in design when:

> The foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the alternative design renders the product not reasonably safe.[105]

While the specific requirements for showing a design defect under a theory of strict liability can vary from state to state,[106] the tests are often similar and usually indistinguishable in the courts' analyses.[107]

---

98. *Id.*

99. *See, e.g.*, Greenman v. Yuba Power Prods., Inc., 377 P.2d 897 (1963) (applying strict liability to claims brought against the manufacturer of an allegedly defective lathe).

100. *See* Restatement (Second) of Torts § 402A(2)(b) (AM. LAW. INST. 1965).

101. *See* Colt, *supra* note 90, at 530, 532.

102. *See* Restatement (Third) of Torts: Products Liability § 2 (AM. LAW. INST. 1998).

103. *See id.*

104. *See* First Amended Complaint, *supra* note 2, at *3.

105. Restatement (Third) of Torts: Products Liability § 2(b) (AM. LAW. INST. 1998).

106. For example, compare Timpte Indus. v. Gish, 286 S.W.3d 306, 311 (Tex. 2009) (explaining that a plaintiff must show "(1) the product was defectively designed so as to render it unreasonably dangerous; (2) a safer alternative design existed; and (3) the

In *Herrick*, the plaintiff alleged "Grindr designed, coded, engineered, manufactured, produced, assembled, and placed" both the Grindr app and Grindr's server-side software into the stream of commerce, and that the app contained "defective conditions and [was] fundamentally unsafe."[108] Herrick alleged that this design defect made the app unreasonably dangerous and caused him to suffer permanent injuries and extreme pain and agony.[109] The court, however, without considering the merits of Herrick's defective design claim, used Section 230 to preclude and dismiss Herrick's claim.[110]

2. Manufacturing Defect

A product contains a manufacturing defect when "the product departs from its intended design even though all possible care was exercised in the preparation and marketing of the product."[111] Unlike a design defect claim, in which the plaintiff seeks to establish that the design of a product was inadequate because the manufacturer failed to use some alternative safer design,[112] a manufacturing defect involves a situation in which the product that caused the injury was allegedly not produced in accordance with the manufacturer's intended design.[113] Similarly to defective design claims, the elements required for proving a manufacturing defect claim vary from state to state; in fact, manufacturing defect's definition can vary over time, even within the

defect was a producing cause of the injury for which the plaintiff seeks recovery"), with Codling v. Paglia, 298 N.E.2d 622, 628–29 (N.Y. 1973) (holding that the manufacturer of a defective product is liable if (1) at the time of injury, the product is being used for the purpose and in the manner normally intended, if (2) the person injured would not through reasonable care have discovered the defect and perceived its danger, and if (3) through reasonable care the person injured or damaged would not otherwise have averted his injury).

107. *See* Kristine Cordier Karnezis, Annotation, *Products Liability: Modern Cases Determining Whether Product Is Defectively Designed*, 96 A.L.R.3d 22, § 2[a] (1979).

108. First Amended Complaint, *supra* note 2, ¶¶ 101, 107.

109. *See id.* ¶¶ 102, 105, 107.

110. *See* Herrick v. Grindr, LLC, 306 F. Supp. 579, 584 (S.D.N.Y. 2019), *aff'd*, 765 Fed. Appx. 586 (2d Cir. 2019).

111. Restatement (Third) of Torts: Products Liability § 2(a) (AM. LAW. INST. 1998).

112. *See* Steven G. Davison, *The Uncertain Search for a Design Defect Standard*, 30 AM. U. L. REV. 643, 643 (1981).

113. *See id.* at 643 n.1. New York courts use a nearly identical test and will find a manufacturing defect "when the specific item that caused the injury does not perform as the manufacturer designed the product-line to perform." LEE S. KREINDLER ET AL., STRICT LIABILITY FOR UNREASONABLY DANGEROUS PRODUCTS—MANUFACTURING DEFECT, NEW YORK PRACTICE SERIES – NEW YORK LAW OF TORTS § 16:19 (2019).

same jurisdiction.[114] The application of these various tests, however, just as with defective design, render largely the same outcome.[115]

Herrick alleged Grindr's app "contained a manufacturing flaw by failing to incorporate widely used, proven and common software to flag and detect abusive accounts that resulted in Grindr selecting and directing an incessant stream [of users] [demanding] sex from [Herrick]," and that these flaws made the Grindr app unreasonably dangerous.[116] Herrick also alleged Grindr's server-side software contained defective conditions that made the app fundamentally unsafe.[117] The court, again relying on Section 230, dismissed Herrick's manufacturing defect claims.[118]

3. Failure to Warn

A failure-to-warn claim arises when a product is defective:

> because of inadequate instructions or warning when the foreseeable risks of harm posed by the product could have been reduced or avoided by the provision of reasonable instructions or warnings by the seller . . . and the omission of the instructions or warnings renders the products not reasonably safe.[119]

Failure-to-warn claims are distinct from both design defect and manufacturing defect claims in that failure-to-warn claims do not allege that the product's design or manufacture was faulty.[120] Rather, failure-to-warn claims arise when a manufacturer fails to provide adequate warning to consumers about foreseeable risks they face in using the product in the way it was intended to be used.[121] Thus, failure-to-warn claims are not "strict liability" in the same way as design defect and manufacturing defect claims because failure-to-warn claims require a factfinder to determine whether a manufacturer acted in accordance with a reasonable standard of conduct.[122] Some states, emphasizing the overlap between negligence and strict liability, apply elements of negligence when

114. *See* David G. Owen, *Manufacturing Defects*, 53 S.C. L. REV. 851, 870 n.108 (2002).

115. *See id.* at 870 ("There are many slight variations in how courts and legislatures define the deviation-from-specification liability standard, although all mean essentially the same thing.").

116. First Amended Complaint, *supra* note 2, ¶¶ 109–10.

117. *See id.* ¶ 112.

118. *See* Herrick v. Grindr, LLC, 306 F. Supp. 579, 584 (S.D.N.Y. 2019).

119. Restatement (Third) of Torts § 2(c) (AM. LAW. INST. 1998).

120. *See* Allan E. Korpela, *Failure to Warn as Basis of Liability Under Doctrine of Strict Liability in Tort*, 53 A.L.R.3d 239, § 2[a] (1973).

121. *See id.*

122. *See id.*

evaluating failure-to-warn claims.[123] Others have rejected this approach.[124]

Herrick asserted a failure-to-warn claim against Grindr based on the premise that Grindr should have warned users that its app could be "used to impersonate and abuse," and "that users can be geographically pinpointed, . . . that the features on the interface to report abusive accounts are merely decorative, and . . . that they shun the basic technology widely used in their industry to prevent or stop known abuse."[125] Herrick also argued, relying on *Doe v. Internet Brands*,[126] that there is "heightened accountability" in an ICS's duty to warn when the product at issue is being used to commit a crime or sexual violence.[127] The court, however, dismissed Herrick's failure-to-warn claim, stating that the *Internet Brands* holding only makes clear that Section 230 does not immunize an ICS from a failure-to-warn claim when the alleged duty to warn arises from something *other* than user-generated content.[128] The court dismissed Herrick's failure-to-warn claim because the content at issue was generated by Herrick's ex-boyfriend, not Grindr.[129]

Thus, the Second Circuit's dismissal of *Herrick* established yet another cause of action from which ICSs are immune.[130] Such expansion of Section 230 creates several problems that negatively impact consumer safety; the remainder of this Comment addresses those problems and proposes that Congress act to protect consumers from significant ICS-inflicted harm.

III. ANALYSIS

Congress passed Section 230 of the Communications Decency Act ("CDA") to achieve several distinct objectives.[131] These objectives

123. *See, e.g.*, Hahn v. Richter, 628 A.2d 860 (Pa. Super. Ct. 1993) (holding that "a manufacturer of prescription drugs is liable only if it fails to exercise *reasonable care* to inform physicians . . . of the facts which make it likely to be dangerous for its intended use" (emphasis added)).

124. *Compare id. with* Patricia R. v. Sullivan, 631 P.2d 91, 102 (Alaska 1981) (holding that it was error to incorporate negligence principles in an instruction as to the need for and adequacy of a warning in a failure-to-warn strict liability action against a manufacturer of electric baseboard heater).

125. First Amended Complaint, *supra* note 2, ¶ 117.

126. Doe v. Internet Brands, 824 F.3d 846, 853 (9th Cir. 2016) (holding that Section 230 did not bar a failure-to-warn claim when a plaintiff was raped by predators who contacted her on a modeling website posing as recruiters and the ICS knew about, but did not warn users about, this danger).

127. *See* Herrick v. Grindr, LLC, 306 F. Supp. 579, 592 (S.D.N.Y. 2019).

128. *See id.*

129. *See id.*

130. *See id.*

131. Congress stated the goal of passing Section 230 was to promote and cultivate both free speech online and the "vibrant free marketplace" on the internet, to incentivize

sometimes intertwine, but as demonstrated by *Herrick*, they often aggravate each other as well.[132] Due to its broad interpretation by most courts, Section 230 insulates ICSs from civil liability so long as the content that caused the alleged injury was created by some third party rather than the ICS itself.[133] This interpretation has created significant concerns for consumer safety, which were left unaddressed by Section 230's drafters.[134]

A. The Herrick *Opinions*

The *Herrick* opinions demonstrate the judicially created vacuum that allows ICSs to shirk their duties to protect consumers solely because the product that they put into the marketplace is an online platform on which users communicate with each other.[135] As noted by Justice Thomas, cases like *Herrick* "were not necessarily trying to hold the defendants liable 'as the publisher or speaker' of third-party content," but instead were trying to allege product-design flaws, which stem from the defendant's own misconduct.[136] However, "courts, filtering their decisions through the policy argument that 'Section 230(c)(1) should be construed broadly,' give defendants immunity."[137]

As shown by *Herrick*, most courts dismiss any civil suit brought against an ICS if the claim could even tangentially fall under Section 230's purview.[138] Because both the Southern District of New York and Second Circuit dismissed Herrick's claims based solely on an overly

---

the use of filtering and blocking technologies to protect children from viewing obscene or objectionable material, and "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer." 47 U.S.C. § 230(a)–(b) (2018).

132. *See generally Herrick*, 306 F. Supp. at 588–92 (holding that Section 230 immunized Grindr from liability despite the plaintiff's allegations that Grindr failed to protect its users from harassment and abuse).

133. *See id.* at 588.

134. *See generally* Goldberg, *supra* note 2; *see also* Citron & Wittes, *supra* note 45, at 463 ("In 1996, it was impossible to foresee the threat to speech imposed by cyber mobs and individual harassers, whose abuse chills the speech of those unwilling to subject themselves to further damage.").

135. *See generally Herrick*, 306 F. Supp. at 590 (concluding, without reference to any supporting evidence, that "[t]here is nothing . . . illegal about Grindr's drop-down menus, its geolocational function, or its sorting, aggregation, and display functions").

136. Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, No. 19-1284, 2020 U.S. LEXIS 4834, at *12 (Oct. 13, 2020) (internal citations omitted).

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

138. *See* Citron & Wittes, *supra* note 45, at 458 ("Courts have built a mighty fortress protecting platforms from any accountability for unlawful activity on their systems—even when they actively encourage such activity or deliberately refuse to address it. The Supreme Court has declined to weigh in on the meaning of Section 230, but state and lower federal courts have reached a near-universal agreement that it should be construed broadly.").

broad interpretation of Section 230's scope, the courts did not analyze Herrick's product liability claims.[139] Neither court determined whether Grindr's geolocation technology reasonably could have been made safer for consumers by comparing the safety of Grindr's technology with safeguards used by its competitors.[140] The courts also did not consider whether Grindr's current technology was designed in a way that put its users at significant risk of harassment and abuse; nor did the courts consider whether Grindr failed to warn its customers of a known risk.[141] These questions were left unanswered because of the courts' choice to immunize Grindr using Section 230 and, as a result, Grindr has no incentive to improve its software to better protect its consumers from harm.[142]

Both *Herrick* opinions, like most opinions analyzing Section 230's scope, completely ignore the foundational policy objectives of the statute—to promote and support the blocking of offensive, obscene, and criminal content.[143] Section 230's protection for "Good Samaritan Blocking" most logically refers to protecting ICSs when they choose to remove offensive or obscene material, as opposed to when ICSs choose not to block material.[144] As previously noted, Congress enacted Section 230 in response to the *Stratton Oakmont*[145] decision and sought to remove a potential disincentive for ISPs to filter and remove objectionable material.[146] Courts, however, have consistently ignored a

139. *See* Jacqueline D. Lipton, *Combatting Cyber-Victimization*, 26 BERKELEY TECH. L.J. 1103, 1132–33 (2011) ("[T]he near-absolute immunity of online service providers under § 230 has in practice prevented courts from engaging in meaningful discussions about the standard of care that might be expected of these service providers absent the statutory immunity.").

140. *See* First Amended Complaint, *supra* note 2, ¶¶ 44–45 (alleging that "Grindr does not utilize proven and common software that would allow it to identify and block abusive users" while "[o]ther similarly situated apps lock out abusive users in the exercise of ordinary care").

141. *See generally id.* ¶¶ 66, 100–120 (averring that Grindr did not warn users that using the app could result in the user becoming a victim of violence).

142. *See* Goldberg, *supra* note 2 ("[L]egal responsibility for one's products and services is the cost of doing business and drives safety innovation.").

143. *See* Haley Halverson, *Ending Immunity of Internet-Facilitated Commercial Sexual Exploitation*, 21 NO. 12 J. INT. L. 3, 6 (2018) ("It is clear that [S]ection 230 of the CDA, while useful to foster Internet growth and speech, has been interpreted in a way that is tone-deaf to its original, contextual purpose. Although the CDA was intended to protect children online, it has ironically been interpreted by the courts to shield facilitators of the commercial sexual exploitation of children, as well as adults.").

144. *See* Doe v. GTE Corp., 347 F.3d 655, 659–60 (7th Cir. 2008); *see also* Amicus Curiae Brief of Consumer Watchdog and Meaghan Barakett in Support of Appellant Herrick and Reversal at *15–16, Herrick v. Grindr, 765 Fed. Appx. 586 (2d Cir. 2019).

145. Stratton Oakmont, Inc. v. Prodigy Servs. Co., INDEX No. 31063/94, 1995 WL 323710 (Sup. Ct. Nassau Cty. May 24, 1995).

146. *See* Machado, *supra* note 33, at 3.

substantial part of Section 230's history.[147] Namely, courts have disregarded the fact that the statute was initially passed in conjunction with legislation that sought to keep obscene and offensive material from being published.[148] Instead, courts have read Section 230 to shield ICSs from liability when they choose not to screen and block offensive material.[149] Such an interpretation eliminates nearly all civil liability for any ICS in most jurisdictions where those claims alleging a failure to block offensive material are brought.[150] As a result, ICSs use Section 230 to avoid responsibility for the danger that their platforms pose to consumers.[151]

1. Section 230 Has Been Used by ICSs to Shirk Their Responsibilities to Consumers

As Chief Judge Kozinski of the Ninth Circuit Court of Appeals explained, "[t]he Communications Decency Act was not meant to create a lawless no-man's land on the Internet."[152] Most courts' current interpretation of Section 230, however, has manifested just that—an environment in which massive online companies, whose businesses have little to do with free expression, may claim Section 230's protections and act with little regard to the risks their products pose to consumers.[153] The

147. *See* Citron & Wittes, *supra* note 45, at 459 ("The judiciary's long insistence that the CDA reflected 'Congress' desire to promote unfettered speech on the Internet' so ignores its text and history as to bring to mind Justice Scalia's admonition against selectively determining legislative intent in the manner of someone at a party who 'look[s] over the heads of the crowd and pick[s] out [their] friends.'" (internal citations omitted)).

148. *See* Cannon, *supra* note 27, at 53.

149. *See, e.g.*, Herrick v. Grindr, LLC, 306 F. Supp. 579, 590 (S.D.N.Y. 2019) (rejecting the plaintiff's argument that Grindr should be responsible for policing and removing impersonating content); *see also* Citron & Wittes, *supra* note 45, at 459.

150. *See* Citron & Wittes, *supra* note 45, at 460.

151. *See, e.g.*, *Herrick*, 306 F. Supp. at 588 (holding that Section 230 provides immunity for Grindr, who allegedly failed to incorporate "widely-used, proven and common software to flag and detect abusive accounts"); *see also* Doe v. Backpage.com, 104 F. Supp. 3d 149, 165 (1st Cir. 2015) (holding that "Backpage.com," a site that offers the services of "escorts," was entitled to Section 230 immunity when it was sued by three underage sex-trafficking victims for facilitating their abuse).

152. *See* Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1164 (9th Cir. 2008).

153. Companies such as AirBnB and eBay have claimed Section 230's protections, despite their business models having little, if anything, to do with facilitating an online platform for free speech. *See generally* Airbnb, Inc. v. San Francisco, 217 F. Supp. 3d 1066 (N.D. Cal. 2016) (denying Airbnb's Section 230 challenge to a city ordinance that makes it a misdemeanor to provide booking services for unregistered rental units); Hinton v. Amazon, 72 F. Supp. 3d 685, 687 (S.D. Miss. 2014) (granting dismissal under Section 230 because "claims against eBay arise or stem from the publication of information on www.ebay.com created by third parties"). Additionally, "[c]urrent day media and tech industry giants, such as the American Society of News Editors, Yelp Inc., and Google,

internet is no longer comprised of small blog-type websites that exist solely as platforms for sharing information online; rather, the internet is now home to many of the largest and most profitable companies in the world.[154] Social networking is a routine part of most Americans' lives, and more people meet romantic partners online than ever before.[155] These massive online companies, however, are insulated from nearly all types of civil liability solely because the product they place into the marketplace is an online platform that relies on the sharing of user-generated content.[156] Section 230's drafters could not possibly have accounted for the sheer number of companies whose profit derives primarily from user-generated online interaction.[157] Section 230, both as written and as it has been interpreted, cannot handle such a fundamental shift in the way the internet is used.[158]

Decisions such as *Herrick* ignore the fundamental dangers posed by a product simply because that product uses third-party-created content to function, thus putting anyone who uses online-dating apps at risk. While some of the risk of online dating cannot be prevented by the dating apps alone, much of it undoubtedly can.[159] Moreover, the choices that dating-

---

have continued to lobby and file suits [sic] appealing to, and supporting, [S]ection 230 immunity of the CDA." Halverson, *supra* note 143, at 11–12.

154. *See generally* Joyce Chepkemoi, *The 25 Largest Internet Companies in the World*, WORLD ATLAS (Apr. 15, 2017), http://bit.ly/31Sd0xo (listing the largest internet companies in the world, as determined by their annual revenue).

155. In 2017, 39% of opposite-sex couples reported that they met online. *See* Michael Rosenfeld et al., Disintermediating Your Friends: How Online Dating in the United States Displaces Other Ways of Meeting 4 (July 15, 2019) (unpublished manuscript), https://stanford.io/2OMhLTy (amended final version published at 116 PROC. OF THE NAT'L ACAD. OF SCI. 17753 (2019)). This percentage is even higher for same-sex couples; 65% of same-sex couples who met in 2017 met online. *See id.* In 1995, around the time Section 230 became law, only 2% of couples reported meeting online. *See* Nick Keppler, *Our Deepest Fears Realized: Most Couples Meet Online Now*, VICE (July 15, 2019, 7:00 AM), http://bit.ly/37nM8pQ.

156. *See* Citron & Wittes, *supra* note 45, at 462 ("If a broad reading of the safe harbor embodied sound policy in the past, it does not in the present—an era in which child (and adult) predation and sexual exploitation on the Internet is rampant, cyber mobs terrorize people for speaking their minds, and actual terrorists use online services to organize and promote their violent activities.").

157. *See generally id.* at 463 ("Now billions of individuals are online in ways that would have been unimaginable when Congress passed the CDA.").

158. *See id.*

159. For example, legislators in the United Kingdom passed legislation requiring the use of age-verification technology for dating apps after *The Sunday Times* found that more than 30 cases of dating app-related child rape have been investigated by UK police since 2015; one of these cases involved a 13-year-old boy with a Grindr profile who was "raped or abused by at least 21 men." Natasha Lomas, *Dating Apps Face Questions Over Age Checks After Report Exposes Child Abuse*, TECHCRUNCH (Feb. 11, 2019, 7:08 AM), https://tcrn.ch/3aMaGvY. While age-verification technology is not a perfect solution to protect all minors who seek access to dating apps, legislators hope it would play a substantial role in keeping children safe from harm. *See id.* ("[A]ge checks, which are

app developers make about whether to put reasonable safety features in place may have especially serious implications for gay men.[160] For example, a survey of 917 men, most of whom were gay, found that "gay and bisexual male users of geosocial dating apps were more than twice as likely as [lesbian, gay, and bisexual] persons generally to be victimized by revenge porn."[161] Among those men who reported being victims of revenge porn, "almost every reported incident of that nonconsensual image sharing occurred on one platform, Grindr."[162]

Grindr users "widely reported that spambots and spoofed accounts run rampant."[163] Indeed, Grindr has established a persistent pattern of ignoring the safety of its users by employing a faulty software design and failing to fix defects that harm users.[164] One study, for example, found that Grindr sends all profile images of users unencrypted across its network and that user locations are sent from devices to the Grindr server with country and city data, with the exact longitude and latitude of users.[165] Grindr also shared both its users' HIV status and location data with third parties for several years.[166] If Grindr has no incentives to develop safeguards to protect its users from harmful or illegal activity perpetuated by other users, then Grindr's failure to protect its consumers will continue, and more app users will be injured as a result.

Interpreting Section 230 to cover all types of civil claims that even indirectly involve some kind of third-party content also eliminates accountability for ICSs who make unsafe products.[167] Gaps in the world of internet and privacy law, enabled by an over-expansive interpretation

---

clearly not without controversy given the huge privacy considerations . . . have also been driven by concern about children's exposure to graphic content online.").

160. *See* Waldman, *supra* note 1, at 988.

161. *Id.* at 988. Revenge porn is "sexually explicit images of a person posted online without that person's consent especially as a form of revenge or harassment." *Revenge Porn*, MERRIAM-WEBSTER.COM DICTIONARY, https://bit.ly/3kwiDJ7 (last visited Sept. 18, 2020).

162. *See* Waldman, *supra* note 1, at 1001.

163. Jon Shadel, *Grindr Was the First Big Dating App for Gay Men. Now It's Falling Out of Favor.*, WASH. POST (Dec. 6, 2018, 12:30 PM), https://wapo.st/2OONgMQ.

164. *See, e.g.*, Devin Coldewey, *Security Flaw in Grindr Exposed Locations to Third-Party Service*, TECHCRUNCH (Mar. 28, 2018, 4:13 PM), https://tcrn.ch/38h1SfL; Azeen Ghorayshi & Sri Ray, *Grindr Is Letting Other Companies See User HIV Status and Location Data*, BUZZFEED NEWS (Apr. 2, 2018, 11:13 PM), http://bit.ly/2RUG4j9.

165. *See* Coldewey, *supra* note 164.

166. *See* Ghorayshi & Ray, *supra* note 164.

167. *See* Ryan Gerdes, *Scaling Back § 230 Immunity: Why the Communications Decency Act Should Take a Page from the Digital Millennium Copyright Act's Service Provider Immunity Playbook*, 60 DRAKE L. REV. 653, 667 (2012) ("Although Congress's intent was to remove disincentives to self-regulation by ISPs—by encouraging ISPs to edit or post third-party material without fear of being regarded as the publisher of the material—§ 230 has failed to provide an incentive for websites to regulate.").

of Section 230, create opportunities for predators to exploit online platforms to harass and injure other users.[168] As demonstrated by Grindr's failure to provide any reasonable safety measures to its users to protect their safety, if ICSs are not incentivized to implement such measures, the problem of stalking, harassment, and sexual violence will only worsen as apps like Grindr become more popular.[169] Broadly dismissing Herrick's claims sends yet another signal to Big Tech that courts are unwilling to protect consumers from harm in the way they have historically done through imposing strict product liability on manufacturers.[170]

B. Product Liability as a Remedy for Dating-App Harassment

Product liability causes of action, such as Herrick's, create an opportunity to hold ICSs accountable when they fail to implement reasonable and widely available measures[171] to protect consumer safety. While the court in *Herrick* did not directly address Grindr's argument that its app is not a "product" for purposes of product liability, the court noted that "it appears to be common ground between the parties that strict product liability may apply to standardized and mass-downloaded software but does not apply to information or 'expressive' content."[172] The distinction between mass-downloaded software and information or expressive content, however, is more difficult to discern if the mass-produced software at issue is designed to facilitate sharing the information or content of its users. For example, Grindr's software

168. *See* Halverson, *supra* note 143, at 6 ("[C]urrent interpretations of [S]ection 230 go beyond reasonable distinctions between third-party posts, and Web site hosts liability to the point of blindly allowing clearly criminal enterprises to continue operating.").

169. *See* Waldman, *supra* note 1, at 988 ("[G]aps in the ecosystem of privacy and Internet law, including privacy tort law, copyright law, criminal law, and the law of platform responsibility governed by [S]ection 230 of the Communications Decency Act, fail to incent privacy-enhancing platform design, thus making revenge porn a feature, not a bug, of online social spaces.").

170. *See* Rushton, *supra* note 93, at 393.

171. In Herrick's case, when his ex-boyfriend began impersonating him on one of Grindr's competitor apps, Scruff, Herrick filed an abuse complaint with Scruff that led to Scruff banning the offending account within 24 hours. *See* Andy Greenberg, *Spoofed Grindr Accounts Turned One Man's Life into a 'Living Hell'*, WIRED (Jan. 31, 2017, 2:57 PM), https://bit.ly/3lB31W2. Scruff also prevented the same device or IP address from creating any new accounts, which Grindr never did. *See id.* Scruff's software also randomizes a user's location if a user elects to hide their distance from other users, so relative distance between users cannot be used to pinpoint a user's exact location. *See* Eric Silverberg, *Location Security & Privacy: An Inside Look*, SCRUFF SUPPORT, https://bit.ly/308YuRW (last visited Sept. 26, 2020). While Herrick's Complaint did not explicitly state which safety measures Grindr could implement, these are a few examples of measures a similar app has taken to protect its users.

172. Herrick v. Grindr, LLC, 306 F. Supp. 3d 579, 592 n.9 (S.D.N.Y 2019).

requires users to input some information in order for the software to function as intended.[173]

Herrick's argument relied on the idea that online-dating apps should be held to the same standards as the manufacturers of any other tangible product.[174] Consumer protections are crucial today because technological developments have created an entirely new universe of risk for consumers of online products.[175] The application of product liability to software is supported by most courts that have addressed the issue.[176] As noted by the court in *Herrick*, many other courts have agreed that product liability can apply to mass-downloaded software.[177] The court's Section 230-based dismissal in *Herrick*, however, leaves unanswered the question of how courts would apply strict product liability when a plaintiff is injured as a result of a defect in a dating app's software.[178]

1. Traditional Product Liability Doctrines Should Apply to Dating-App Software

Some basic assumptions can be made about how traditional product liability could apply to dating apps. If a court were to apply a risk-utility test,[179] to avoid liability, dating apps would need to show that the economic cost of implementing more thorough safety measures in the app's software was higher than the risk of danger created by the app's current software design.[180] Alternatively, if a court were to apply a

173. *See generally id.* at 589 (citing Dyroff v. Ultimate Software Grp., Inc., No. 17-CV-5359-LB, 2017 WL 5665670, at *10 (N.D. Cal. Nov. 26, 2017) (explaining that it is "the users' voluntary inputs that create the content . . . not [defendant's] proprietary algorithms") (alteration in original)).

174. *See* First Amended Complaint, *supra* note 2, ¶ 88 ("Upon information and belief, despite having copious resources to do so, Grindr does not invest in the safety of its product, and does not prioritize the safety of its users over its own profit.").

175. *See Herrick*, 306 F. Supp. at 584–85 (where the plaintiff was the victim of a Grindr-facilitated, months-long campaign of abuse and harassment); *see also* Doe v. Internet Brands, 824 F.3d 846, 848–49 (9th Cir. 2016) (where the plaintiff was drugged, raped, and recorded after being "scouted" by predators on a site called "ModelMayhem.com"); Doe v. Backpage.com, 104 F. Supp. 3d 149, 151–53 (1st Cir. 2015) (where "Backpage.com," a site that offers the services of "escorts," was unsuccessfully sued by three underage sex-trafficking victims for facilitating their abuse).

176. *See Herrick*, 306 F. Supp. at 592 n.9; Schafer v. State Farm Fire & Cas. Co., 507 F. Supp. 2d 587, 601 (E.D. La. 2007) (holding that computer software is a "product" for purposes of product liability); *see also* Winter v. G.P. Putnam's Sons, 938 F.2d 1033, 1035 (9th Cir. 1991) (suggesting that computer software could be considered a "product" for purposes of product liability).

177. *See Herrick*, 306 F. Supp. at 592 n.9.

178. *See generally id.* at 588–92 (declining to discuss Herrick's product liability claims after deciding that Grindr was immune under Section 230).

179. *See* Colt, *supra* note 90, at 530, 532 (explaining that a risk-utility test balances the benefits of avoiding a safety risk with the costs of doing so).

180. *See* Restatement (Third) of Torts: Products Liability § 2 (AM. LAW. INST. 1998).

consumer expectations test,[181] to avoid liability, dating apps would need to implement available technology so that their apps were not unreasonably dangerous to consumers.[182] In either case, the very nature of the tests courts use to evaluate product liability claims ensures that dating apps would not be unduly burdened by requirements to account for and attempt to prevent every single possible injury that could occur.[183]

Speech by a third party on an online platform, by itself, would also not be enough to give rise to a civil lawsuit.[184] Under Section 230, only those claims in which the plaintiff can show that the injury was a result of a defective warning or defect in the app's software would survive.[185] For example, in *Herrick*, the plaintiff argued that the alleged injury was not the result of any third-party content posted to the Grindr app, but was instead caused by Grindr's allegedly faulty software design.[186] In other situations, poorly designed software could potentially allow hackers and other bad actors to gain access to and share damaging or sexually explicit information from users that put it onto the app with the expectation that the information would be secure.[187] Such a defect could be particularly disastrous for lesbian, gay, bisexual, and other queer dating app users.[188] If those bad actors gained access to the users' sensitive information due to weaknesses in the software's design or the app's failure to implement available safety features, product liability could be a possible route of litigation for victims. Such claims would focus on the design of the

181. *See* Colt, *supra* note 90, at 530, 532 (explaining that the consumer expectations test focuses on whether a product fails to meet the safety expectations of an ordinary consumer).

182. *See Consumer Expectations Test*, LEGAL INFO. INST., https://bit.ly/38SD6We (last visited Jan. 10, 2020).

183. *See generally* 2 Louis R. Frumer and Melvin I. Friedman, *Products Liability* § 11.03 (2020) (describing available defenses to product liability actions).

184. *See id.* ("[A] plaintiff must prove that the product's defective design caused his or her injury.").

185. *See id.*

186. *See* First Amended Complaint, *supra* note 2, ¶ 49.

187. For example, in 2018, a security flaw in Grindr's app exposed the location data of its more than three million daily users. *See* Brian Latimer, *Grindr Security Flaw Exposes Users' Location Data*, NBC NEWS (Mar. 28, 2018, 7:52 AM), https://nbcnews.to/2SRnFEv. This leak even exposed the location data of people who opted out of sharing their location information. *See id.* The person who exposed the leak, Trever Faden, said, "one could, without too much difficulty or even a huge amount of technological skill, easily pinpoint a user's exact location." *Id.*

188. *See id.* ("Location data for Grindr users is particularly sensitive. Grindr has users in 234 countries and territories around the world. Homosexuality is illegal in more than 70 nations, and 13 of them implement the death penalty for homosexual acts, according to a 2016 report by the International Lesbian, Gay, Bisexual, Trans and Intersex Association (ILGA).").

software in question, rather than on any third-party content that users put onto the app.

One major obstacle for bringing product liability claims against apps, however, is that most courts require that the plaintiff suffer a physical injury or damage to property.[189] In *Hayes v. SpectorSoft Corp.*,[190] for example, the United States District Court for the Eastern District of Tennessee found that emotional injuries alone were insufficient grounds for bringing a product liability action against an app.[191] Consequently, relatively few injuries that could feasibly arise from using an app would be compensable under traditional product liability if courts, like in *Hayes*, fail to provide remedies for emotional injuries.

Some apps, however, may be liable if a physical injury results from its defective software. For example, in 2016, news outlets widely reported various car accidents and physical injuries that users of the "Pokémon Go" app suffered while using the app.[192] Scholars have also assessed the potential for product liability claims against the manufacturers of software for automated vehicles, products that can easily cause physical injury.[193]

Dating apps similarly pose a heightened risk of causing real, physical harm to users.[194] The plaintiff in *Herrick*, for example, endured an "endless stream of horny and violent strangers" that exposed him to a continuous threat of physical injury.[195] Weak and easily manipulated geolocation technology, as alleged in *Herrick*, as well as unencrypted sensitive personal information of users, expose dating-app users to significant risk of physical injury by bad actors who obtain their personal information.[196] If app developers are not incentivized to implement available technology to protect against such foreseeable risks, dating-app

189. *See* Frumer & Friedman, *supra* note 183, § 13.03 ("Courts in most jurisdictions still deny recovery for emotional injury in the absence of some existing physical effect.").

190. Hayes v. SpectorSoft Corp., No. 1:08-cv-187, 2009 WL 3713284 (E.D. Tenn. Nov. 3, 2009).

191. *See id.* at *31.

192. *See* Philip Quaranta, *Pokemon GO: An Indicator of Product Liability in the App Economy*, LEXOLOGY (Aug. 19, 2016), http://bit.ly/35EuoFO.

193. *See, e.g.*, Sunghyo Kim, *Crashed Software: Assessing Product Liability for Software Defects in Automated Vehicles*, 16 DUKE L. & TECH. REV. 300, 300 (2017).

194. *See, e.g.*, Herrick v. Grindr, LLC, 306 F. Supp. 579, 584–85 (2d. Cir. 2018) (where a dating app was used to facilitate a campaign of harassment against an ex-boyfriend).

195. First Amended Complaint, *supra* note 2, ¶ 9.

196. *See generally* Coldewey, *supra* note 164 (stating that Grindr shared the location of its users with third parties without consent); *see also Herrick*, 306 F. Supp. at 585 (alleging that geolocation spoofing was used to send Grindr users to the plaintiff's location).

users will continue to be put in danger and will have no means of seeking legal recourse against an app if they are injured.

Although product liability alone is an insufficient remedy to end all types of dating-app harassment, it nonetheless could be a viable cause of action when an app's software is so defectively designed that it can be easily manipulated to find and harass another user or to gain sensitive information about a user. If app developers could face product liability litigation for failing to implement reasonable safety features to protect consumers, app developers would be incentivized to find more innovative ways to protect their users from harm.

Apps would have several potential means of defending themselves against product liability suits. Apps could claim that their product was unforeseeably misused.[197] Such a defense precludes claims when the product at issue was used "in a capacity which is unforeseeable and incompatible with the product's design"; such could be the case if a bad actor significantly manipulated an app's software to cause injury.[198] This defense, however, would be contingent on the misuse of the app being *unforeseeable*, a factual inquiry for a court or jury to undertake.[199] Proving unforeseeable misuse would be challenging for an app because developers routinely foresee hacking when designing software and take proactive steps to ensure the app software is not misused.[200] Alternatively, an ICS could claim that its product was altered or modified after the ICS created the software and put it into the marketplace for consumer use, which courts often view as a complete defense to product liability claims.[201] Nonetheless, lawmakers must design laws to incentivize apps to take reasonable steps to protect their users.

While product liability could be a powerful tool for protecting consumers from the dangers of dating apps, as demonstrated by *Herrick*, Section 230 prevents courts from performing any meaningful analysis of claims like the ones plead by Herrick.[202] With the exception of the

197. *See* Quaranta, *supra* note 192 (speculating that the Pokémon GO app developers could argue their app was unforeseeably misused if facing product liability claims).

198. David Oberly, *Utilizing the Unforeseeable Misuse Defense to Dispose of Product Liability Claims*, 12 Q. REV. OHIO ASSOC. CIV. TRIAL L. 6, 6 (2018).

199. *See id.*

200. *See id.* at 6 ("Only those circumstances which the manufacturer perceived or should have perceived at the time of its respective actions should be considered.").

201. *See* 1 Louis R. Frumer and Melvin I. Friedman, *Products Liability* § 8.04 (2020).

202. *See generally* Herrick v. Grindr, LLC, 306 F. Supp. 579, 584 (S.D.N.Y. 2019), *aff'd*, 765 Fed. Appx. 586 (2d Cir. 2019) (barring the plaintiff from bringing product liability claims against the defendant due to Section 230's broad civil immunity for ICSs).

Seventh[203] and Ninth Circuits,[204] most appellate courts have refused to recognize any notable exceptions to the overly broad scope of Section 230.[205] Thus, unless Congress acts to amend Section 230, Section 230 will likely continue to be a monumental barrier for plaintiffs bringing product liability suits against app developers when the app's primary function is to facilitate the sharing of information or content between its users.

C. Opportunities for Legislative Action

The contemporary online landscape has created a plethora of difficult issues that Section 230's drafters could not possibly have foreseen.[206] Online dating has pitted free speech and consumer safety against each other.[207] Due to Section 230's broad interpretation, companies operating online products used by consumers for communicating with others are essentially insulated from any kind of product liability solely due to the nature of their products.[208] If courts are

---

203. *See* Chi. Lawyers' Comm. For Civ. Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008) (stating that "[Section] 230(c) as a whole cannot be understood as a general prohibition of civil liability for web-site operators and other online content hosts"); *see also* Doe v. GTE Corp., 347 F.3d 655, 659 (7th Cir. 2003).

204. *See generally* Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008) (holding that an ICS can be liable for third-party content posted on its platform if the ICS materially contributed to what made that content illegal or objectionable). The Ninth Circuit's willingness to create exceptions for Section 230's broad interpretation is significant, given the Circuit's jurisdiction over San Jose and Silicon Valley, which had the largest concentration of high-tech jobs in 2018. *See* Richard Florida, *America's Tech Hubs Still Dominate, but Some Smaller Cities Are Rising*, CITYLAB (Apr. 18, 2019), http://bit.ly/39P1PZT. The San Francisco-Silicon Valley Area received nearly 46% of all venture capital investments in 2018, signifying that Big Tech's presence in the Ninth Circuit's jurisdiction will only continue to grow. *See* Justin Fox, *Venture Capital Keeps Flowing to the Same Places*, BLOOMBERG OPINION (Jan. 8, 2019, 10:00 AM), https://bloom.bg/2N9d8T2.

205. *See Herrick*, 306 F. Supp. at 584; *see also* Doe v. Backpage.com, 104 F. Supp. 3d 149, 165 (1st Cir. 2015) (holding that "Backpage.com," a site offering the services of "escorts," was entitled to Section 230 immunity when it was sued by three underage sex-trafficking victims for facilitating their abuse); Jones v. Dirty World Entm't Recordings, LLC, 755 F.3d 398 (6th Cir. 2014) (refusing to provide Section 230 immunity to a site which editorialized on anonymous, allegedly-defamatory posts from third-party users); Green v. America Online (AOL), 318 F.3d 465 (3d. Cir. 2003) (finding that Section 230 does not require an ICS to restrict speech, but instead "allows an ICS to establish standards of decency without risking liability for doing so").

206. *See* Citron & Wittes, *supra* note 45, at 463 ("At the most basic level, the [technology] companies and their successors are vastly larger, more powerful, and less vulnerable than were the nascent 'online service providers' of two decades ago. They are also providing services very different from, and less obviously about speech, than the Prodigy-like services that Congress sought to protect.").

207. *See id.*

208. *See, e.g.*, *Herrick*, 306 F. Supp. at 601 (dismissing Herrick's suit against Grindr).

unwilling to interpret Section 230's scope more reasonably to rein in ICS immunity and thereby protect dating-app users, Congress must act to amend Section 230. Such reform is crucial for incentivizing ICSs to make their technology safe for consumers and for holding ICSs accountable when they fail to do so.[209]

To solve the problem of dating-app violence, several scholars have recommended that Congress criminalize revenge porn at the federal level.[210] While such an approach may have a positive impact in reducing instances of revenge porn, it would likely have little effect on cases like *Herrick*, where a dating app was used to facilitate in-person harassment.[211] Criminalizing revenge porn, on its own, would also provide only limited incentives to ICSs to implement changes that make their platforms safer. While ICSs would likely implement stronger protocols to identify and block revenge porn, they would not be similarly incentivized to account for other potential forms of abuse—such as harassment and stalking—that could occur due to defects in their software.[212]

Another broader legislative approach proposed by scholars reads:

> No provider or user of an interactive computer service that *takes reasonable steps to prevent or address unlawful uses of its services once warned about such uses* shall be treated as the publisher or speaker of any information provided by another information content provider *in any action arising out of the publication of content provided by that information content provider*.[213]

This "reasonable steps" approach, however, makes no distinction between torts involving publication—such as defamation, libel, and slander—and other torts like negligence, invasion of privacy, misappropriation, and product liability.[214] Consequently, the approach may prioritize one objective of Section 230—encouraging blocking and filtering offensive content—at the expense of Section 230's other objective—promoting free speech and a free online marketplace.[215] The

209. *See* Coldewey, *supra* note 164; *see also Herrick*, 306 F. Supp. at 585 (alleging that geolocation spoofing was used to send Grindr users to the plaintiff's location).

210. *See, e.g.*, Waldman, *supra* note 1, at 1007.

211. *See Herrick*, 306 F. Supp. at 584–85.

212. *See generally* Waldman, *supra* note 1, at 1008 (concluding that, in addition to the criminalization of revenge porn, "modest reform to Section 230 would also help" remedy problems with sexual assault, harassment, and rape in gay online communities).

213. Citron & Wittes, *supra* note 45, at 471.

214. *See generally Immunity for Online Publishers Under the Communications Decency Act*, DIGITAL MEDIA L. PROJECT, http://bit.ly/2SS05Yf (last visited Jan. 12, 2020) (explaining that Section 230 immunity has been found in claims alleging defamation, invasion of privacy, misappropriation, and negligence).

215. *See* 47 U.S.C. § 230(a)–(b) (2018).

proposed approach also requires ICSs to determine what constitutes an unlawful use of its services.[216] Resting the responsibility on ICSs to determine whether content is unlawful under a statute may be so burdensome for them that, fearful of facing liability, ICSs may inadvertently choose to remove content that was actually put online legally.[217]

The best possible way for legislators to protect dating-app users is to clarify which causes of action Section 230 was intended to include. Congress has already exempted federal criminal law,[218] intellectual property law,[219] and communications privacy law[220] from the protections of Section 230. In 2018, Congress also passed the Fight Online Sex Trafficking Act ("FOSTA"),[221] which (1) clarifies that Section 230 does not prohibit the enforcement against ICSs of criminal and civil sex-trafficking laws, and (2) criminalizes the promotion or facilitation of prostitution and reckless disregard of sex trafficking.[222] While FOSTA has drawn significant criticism for its effect on vulnerable populations,[223] the legislation functions in a way that keeps the core principles of Section 230 intact while adding an important caveat that keeps ICSs from using Section 230's significantly expanded scope to escape liability for facilitating and promoting sex trafficking.[224]

---

216. *See* Citron & Wittes, *supra* note 45, at 471.

217. For example, many of FOSTA's opponents point out that websites frequently remove explicit content that they fear would violate FOSTA when in reality, the content was voluntarily and legally put online. *See* Elliot Harmon, *How Congress Censored the Internet*, ELECTRONIC FRONTIER FOUND. (Mar. 21, 2018), http://bit.ly/2U4Pb3c ("[F]acing the risk of ruinous litigation, online platforms will have little choice but to become much more restrictive in what sorts of discussion—and what sorts of users—they allow, censoring innocent people in the process.").

218. *See* 47 U.S.C. § 230(e)(1).

219. *See id.* § 230(e)(2).

220. *See id.* § 230(e)(4).

221. 18 U.S.C. § 2421A (2018). FOSTA is often referred to in conjunction with the Stop Enabling Sex Traffickers Act ("SESTA"). *See* Lura Chamberlain, *FOSTA: A Hostile Law with a Human Cost*, 87 FORDHAM L. REV. 2171, 2173 n.6 (2019). While the bills were not identical, Congress "effectively subsumed SESTA into FOSTA prior to the latter's enactment." *Id.* (citing 164 Cong. Rec. H1248 (daily ed. Feb. 26, 2018)).

222. *See* 18 U.S.C. § 2421(A).

223. FOSTA has been heavily criticized for putting sex workers who rely on the internet at risk, as it essentially forces them off a safer platform for soliciting clients and requires them to resort to less safe, in-person methods of finding work. *See* Karol Markowicz, *Congress' Awful Anti-Sex-Trafficking Law Has Only Put Sex Workers in Danger and Wasted Taxpayer Money*, BUS. INSIDER (July 14, 2019, 8:38 AM), http://bit.ly/37rLHeZ. Critics also argue that the law's broad wording has forced ICSs to remove lawful content. *See also* Romano, *supra* note 74.

224. FOSTA's language amends Section 230 to clarify that nothing in Section 230's text "shall be construed to impair or limit (a) any claim in a civil action" that is brought against a party for "manag[ing], or operat[ing] an [ICS] . . . with the intent to promote or facilitate the prostitution of another person." The Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164 (2018).

Lawmakers should employ a FOSTA-like structure for any amendments that exclude product liability suits from Section 230's protections. Such an approach would clarify that Section 230 does not prevent ICSs from incurring liability when an alleged injury was the result of a defect in the design or manufacture of their software.[225] Further, the approach would keep the fundamental purposes of Section 230 intact while still incentivizing ICSs to provide stronger consumer protections.[226] Given the limitations of traditional product liability,[227] an amendment allowing ICSs to be sued on a product liability theory would also be narrow enough to avoid endless liability for ICSs. Data breaches,[228] for example, likely would only be actionable if the victim of the alleged breach incurred some direct, physical injury or damage to property from the breach; therefore, most traditional data breaches would be non-actionable under this proposed provision.[229]

Limiting the scope of Section 230's immunity is crucial to hold massive, internet-based companies liable for their failures to adequately protect their consumers. Allowing plaintiffs to bring product liability suits against these companies would incentivize innovation and protect consumers, while keeping Section 230's protections for internet speech intact.

IV. CONCLUSION

The *Herrick* opinions display the ever-widening chasm that has emerged between federal law and online-platform safety.[230] While

---

225. *See id.*

226. *See generally* Halverson, *supra* note 143, at 7 ("These current interpretations have obvious consequences when Web sites are disincentivized from investing serious resources to monitoring their Web site for criminal content. . . . [I]t is more economically prudent for a Web site to simply rely on the effectively guaranteed [S]ection 230 immunity than to police their Web sites for criminal activity.").

227. *See* Frumer & Friedman, *supra* note 194, § 13.03 ("Courts in most jurisdictions still deny recovery for emotional injury in the absence of some existing physical effect.").

228. "A data breach occurs when there is an unauthorized entry point into a corporation's database that allows cyber hackers to access customer data such as passwords, credit card numbers, Social Security numbers, banking information, driver's license numbers, medical records, and other sensitive information" for purposes of committing identity theft or fraud. Nicole Martin, *What Is a Data Breach?*, FORBES (Feb. 25, 2019, 12:27 PM), http://bit.ly/38JRVrc. Civil claims over data breaches are typically brought as negligence actions. *See* Michael Ruttinger, *Lessons for Data Breach Lawyers From Product Liability*, LAW360 & TUCKER ELLIS LLP (Jan. 26, 2018, 11:09 AM), http://bit.ly/3aGhICe.

229. *See generally* Ruttinger, *supra* note 228, at *2 (noting that the economic loss doctrine has been applied to data-breach claims).

230. *See generally* Herrick v. Grindr, LLC, 306 F. Supp. 579, 584, 585–86, 601 (S.D.N.Y. 2019) (dismissing a suit against Grindr when a bad actor used weaknesses in the app's software to victimize the plaintiff).

Section 230 of the Communications Decency Act has allowed the internet to flourish into a bastion of free speech,[231] the internet has grown to an extent unimaginable to the statute's original drafters.[232] As demonstrated by *Herrick*, the internet's pervasiveness in every-day life has created new problems that threaten consumers' lives and safety.[233] Meanwhile, Section 230's protections have been progressively expanded to bar nearly every type of civil claim against an ICS simply because some kind of third-party content was involved in the injury.[234] Not only does such an expansive interpretation of Section 230 run contrary to Congress's intent in passing the statute, it also ignores the massive consumer safety concerns inherent in the modern internet landscape.[235]

Because courts will likely fail to scale back their own broad interpretation of Section 230, Congress is in the best position to put reasonable limitations on Section 230's scope.[236] An amendment to Section 230 allowing plaintiffs to sue when their injuries were caused by a defect in the design or manufacture of software would protect consumer safety while still preserving the important speech protections that the statute affords.[237]

231. *See Section 230 of the Communications Decency Act*, ELECTRONIC FRONTIER FOUND., https://bit.ly/3pvN8CL (last visited Feb. 15, 2020) (calling Section 230 one of "the most valuable tools for protecting freedom of expression and innovation on the Internet").

232. *See supra* Section III.A.1.

233. *See supra* Section III.A.1.

234. *See supra* Section II.B.

235. *See supra* Section III.A.1.

236. *See supra* Section III.C.

237. *See supra* Section III.C.