The Case for a Safe Harbor Provision of CDA 230 That Allows for Injunctive Relief for Victims of Fake Profiles*

Camille Bachrach*

TABLE OF CONTENTS

*This Note was written before President Trump's Executive Order issued on May 28, 2020—"Executive Order on Preventing Online Censorship"—and does not contemplate, analyze, or incorporate any suggestions or proposals made in the Executive Order. Additionally, this Note does not account for any regulations or clarifications promulgated by the Federal Communications Commission about Section 230 of the Communications Decency Act per the Exeuctive Order's directive.

*J.D., May 2020, The George Washington University Law School; B.S., Magazine Journalism, B.A., Political Science, Concentration: Law & Politics, May 2015, Syracuse University. Articles Editor, Federal Communications Law Journal, Vol. 72. Thank you to the Federal Communications Law Journal (FCLJ), FCLJ Adjunct Meredith Rose, and FCLJ Faculty Advisor Professor Dawn Nunziato for their invaluable help, advice, and assistance with transforming an idea into a Note. I would also like to thank my parents, Carlos and Deborah, and my brother, Kevin, for the unconditional love and support throughout the past three years—I couldn't have done law school without them.

I. INTRODUCTION

You join a dating app in hopes of meeting a new fling or love interest, or maybe in hopes of entering into a serious relationship. You swipe a lot. Then you swipe some more. You finally match with someone, and after a few months of talking and dating, you decide to be exclusive. So, you deactivate your dating profile, as it has successfully fulfilled its purpose. Unfortunately, some love stories are not destined to last forever, and your new relationship ends the following year. Right around that time, your ex begins impersonating you on the very app you met on. He creates profiles bearing your actual name with real photos—but lying about almost everything else.

Your new profile now says that you are "interested in 'serious kink and many fantasy scenes[]' [and] hardcore and unprotected group sex" among other things.[1] In the span of six months, about 1,100 people respond to this profile.[2] You try and report it to the dating app, but the only response you receive is an "automated, form response,"[3] lacking a recommended remedy—and, more importantly, lacking a promise to delete all the fake profiles. So, what can you do? After the Second Circuit Court of Appeals' ruling on March 27, 2019 in *Herrick v. Grindr*[4]—nothing.

This hypothetical situation reflects some of the facts from *Herrick v. Grindr*.[5] Last year, the Second Circuit Court of Appeals issued a decision in this case that created yet another way in which interactive computer services are broadly protected by the Communications Decency Act's Section 230

1. Herrick v. Grindr, LLC., 306 F. Supp. 3d 579, 585 (S.D.N.Y. 2018) (quoting Pl.'s Am. Compl. ¶ 50).

2. *Id.* (quoting Pl.'s Am. Compl. ¶ 49).

3. *Id.* (quoting Pl.'s Am. Compl. ¶ 71).

4. Herrick v. Grindr LLC., 765 F. App'x 586 (2d Cir. 2019), *cert. denied*, 140 S. Ct. 221 (2019). The Second Circuit ruled that Grindr, as an interactive computer service, was not responsible for the content posted on its application by third parties. *Id.* Previously, the Southern District of New York also stated that Grindr was immunized from Herrick's claims under Section 230 of the Communications Decency Act, 47 U.S.C. § 230(c)(1) (2018), as that Section shields "Grindr from liability for content created by other users." *Herrick*, 306 F. Supp. 3d at 584. Additionally, the court denied Herrick's application to renew a temporary restraining order that was previously entered in New York State Supreme Court (before the case was moved to federal court). *See* Op. and Order at *1, Herrick v. Grindr, LLC., 17-CV-932, 2017 WL 744605 (S.D.N.Y. 2017).

5. *Herrick*, 306 F. Supp. 3d at 585.

(hereinafter CDA 230)[6] and leaves future defrauded individuals with almost no useful remedies.[7]

CDA 230 immunizes interactive computer services from liability by protecting them from being "treated as the publisher or speaker of any information provided by another information content provider."[8] While legislative history, as well as the additional effects of CDA 230, will be covered in more detail in Sections III, IV, and V of this Note, a brief overview will be useful before reading the facts of *Herrick v. Grindr* below.[9]

CDA 230 creates protections for providers of "interactive computer service[s]"[10] by not treating them as the original publisher or speaker of content posted by users on their platform.[11] The Act also imposes no liability if they chose not to monitor or restrict access to content considered to be "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable,"[12] or, alternatively, if they take any action that "enable[s] and make[s] available to information content providers[13] or others the technical means to restrict access to"[14] such content.

Most courts have interpreted the Act's requirement of "impos[ing] no liability" to mean that in claims against an interactive computer service,

---

6. *Id.* (affirming No. 18-396, 2019 WL 1384092, at *5 (2d. Cir. March 27, 2019)).

7. *Herrick*, 765 F. App'x at 586; *see* 47 U.S.C. § 230(c)(1) (2018). Under CDA 230, courts have taken the phrase "no liability" to bar injured plaintiff's from seeking injunctive relief. *See* Medytox Solutions, Inc. v. Investorshub.com, Inc., 152 So. 3d 727, 731 (Fla. Dist. Ct. App. 2014) ("Thus, by the plain language of the statute, the immunity afforded by [S]ection 230 encompasses the claims for declaratory and injunctive relief sought in the case."); Smith v. Intercosmos Media Group, Inc., No. Civ. A.02-1964, 2002 WL 31844907 at *4 (E.D. La. 2002) ("This Court . . . concludes that any claim made by the plaintiffs for damages or injunctive relief with regard to either defamation and libel, or negligence and fault under Article 2315, are precluded by the immunity afforded by Section 230(c)(1), and subject to dismissal."). Thus, by not allowing injunctive relief for plaintiff's suing interactive computer services that are immune under CDA 230, when the claim relates to fake profiles, the plaintiff is currently left with no viable recourse, for if the interactive computer service does not voluntarily remove the profile, a court cannot require them to. *See* Hassell v. Bird, 420 P.3d 776, 779 (Cal. 2018) (stating that a lower court's order requiring Yelp to remove the contested reviews was "improperly treat[ing] Yelp as 'the publisher or speaker of [] information provided by another information content provider" and this is the exact thing that CDA 230 immunizes interactive computer providers from).

8. 47 U.S.C. § 230(c)(1) (2018).

9. *Herrick*, 306 F. Supp. 3d at 585.

10. 47 U.S.C. § 230(c)(1) (2018); § 230(f)(2).

11. 47 U.S.C. § 230(c)(1) (2018).

12. 47 U.S.C. § 230(c)(2)(A) (2018).

13. Typically, an information content provider is the individual or entity that creates or develops the content.

14. *Id.* § 230 (c)(2)(B). *See* Adi Kamdar, *EFF's Guide to CDA 230: The Most Important Law Protecting Online Speech*, Electronic Frontier Foundation (Dec. 6, 2012), https://www.eff.org/deeplinks/2012/12/effs-guide-cda-230-most-important-law-protecting-online-speech [https://perma.cc/TS8M-GXFF] ("Websites could edit, filter, and screen content if they wanted without being held liable for the content itself.").

injunctive relief cannot be sought.[15] However, this Note will argue that there should be an exception to this immunity for cases of fraud and impersonation. This exception would allow for CDA 230 immunity to be available in these circumstances only if certain requirements are met and a reasonableness requirement is satisfied. If the plaintiff is successful in this showing, then injunctive relief can be a viable option, as one factor that injunctive relief is dependent on is the likelihood of success on the merits of the case.[16] By amending CDA 230 to add this exception, Congress will be changing the requirements of CDA 230 immunity for cases of fraud and impersonation, thus altering the availability of CDA 230 immunity for these types of cases. This Note will advance this exception by using the facts of *Herrick v. Grindr*[17] as a framework for a situation where the proposed exception would have readily applied and could have been a helpful remedy for the plaintiff.

Section II will provide an overview of the facts of *Herrick v. Grindr.*[18] Section III will introduce CDA 230 and provide background information for the context of the statute's promulgation and its effects. Section IV will discuss cases concerning fake profiles, CDA 230 immunity, and how the courts have resolved those cases. Section V will provide an overview of the viability and inconsistency of grants of injunctive relief when CDA 230 is being used to immunize an interactive computer service. Additionally, it analyzes whether fraud and impersonation are covered by CDA 230 by looking at congressional intent, legislative history, and differentiating fraud and impersonation from defamation claims. Section VI will introduce the proposed exception for cases of false impersonation when CDA 230 should not apply and thus injunctive relief can be granted.

---

15. *See* Medytox Solutions, Inc. v. Investorshub.com, Inc., 152 So. 3d 727, 731 (Fla. Dist. Ct. App. 2014) ("[T]he immunity afforded by [S]ection 230 encompasses the claims for declaratory and injunctive relief sought in the case."). *But see* Mainstream Loudoun v. Board of Trustees of Loudoun County Library, 2 F. Supp. 2d 783, 790 (E.D. Va. 1998) ("[D]efendants cite no authority to suggest that the 'tort-based' immunity to 'civil liability' described by § 230 would bar the instant action, which is for declaratory and injunctive relief.") (citing 47 U.S.C. § 230(a)(2) (2018); *Zeran*, 129 F.3d at 330.). The court explicitly held that Section 230 does not bar an action for injunctive relief. *Mainstream Loudoun*, 2 F. Supp. 2d at 790.

16. *See* Op. and Order at 3, Herrick v. Grindr, 17-CV-932 (VEC), 2017 WL 744605 (S.D.N.Y. Feb. 24, 2017) (*citing* MyWebGrocer, LLC v. Hometown Info., Inc., 375 F.3d 190, 192 (2d Cir. 2004)). This Note proposes that by altering the underlying requirements that a plaintiff has to satisfy in order to obtain CDA 230 immunity, the merits of the case also change—rendering a different outcome in courts when plaintiffs request for injunctive relief.

17. Herrick v. Grindr LLC., 765 F. App'x 586 (2d Cir. 2019).

18. *Id.*

II. FACTS OF *HERRICK V. GRINDR*

Around May 2011, Matthew Herrick[19] joined Grindr[20] and used the app for several years until he and a man named JC began talking and dating around June 2015.[21] In November 2015, Herrick removed his profile off Grindr, as he and JC were becoming more serious.[22] Soon after, JC began impersonating Herrick on Grindr—using a fake profile to talk with other users.[23] However, in June 2016, Herrick found out and successfully convinced JC to stop impersonating him.[24] In August 2016, Herrick began using his personal Grindr account again, and subsequently broke off his relationship with JC around October 2016 due to "JC's abuse and control."[25]

Once more, JC created a fake Grindr profile impersonating Herrick and this time scheduled "appointments for sexual encounters" between Herrick and other strangers.[26] JC would "manipulate the geo-physical settings"[27] to correspond with Herrick's home and work location and talk to men on the app in order to set up "sex dates" between them and Herrick.[28] JC would tell people that he (acting as Herrick) wanted to have sex and told them where to find him.[29] JC would also tell men on Grindr to "expect [Herrick's] resistance as part of an agreed upon rape fantasy or role play" which added even more danger to Herrick's life.[30] Herrick didn't feel safe inside his own home, had men bang on his window demanding to see him, and had some men refuse to leave "until they were physically escorted off the premises."[31]

Dozens of men have shown up at Herrick's work and apartment "expecting to have sex" with him and even refusing to leave when Herrick

19. Matthew Herrick was around 26 years old. Pl.'s Compl. at 2, Herrick v. Grindr, No. 150903/2017 (N.Y. Sup. App. Div., Jan. 27. 2017).

20. Founded in 2009, Grindr is a popular dating app for gay men. *See* Katerina Ang, *Why Pioneering Dating App Grindr Hopes to Become a Big-Time Media Publisher*, MARKET WATCH (Dec. 30, 2017), https://www.marketwatch.com/story/why-pioneering-dating-app-grindr-hopes-to-become-a-big-time-media-publisher-2017-12-30 [https://perma.cc/U67F-DK9S].

21. Pl.'s Compl. at 9-10, *Herrick*, No. 150903/2017.

22. *Id.* at 10.

23. *Id.*

24. *Id.*

25. *Id.*

26. *Id.*

27. Normally, Grindr tracks a user's geolocation (a precise identification or a rough estimate of the location of the user), and based on that location, Grindr organizes matches on the App from "nearest to furthest." Pl.'s First Am. Compl. at 5, *Herrick*, No. 150903/2017. However, in this case, Herrick claims that JC would manipulate the automatic geolocation setting on the App to reflect Herrick's work and home address instead of JC's location. Pl.'s Compl. at 12, *Herrick*, No. 150903/2017.

28. Pl.'s Compl. at 12, *Herrick*, No. 150903/2017.

29. *See id.*

30. *Id.* at 14.

31. *Id.*

told them his profile is not him but merely an impersonation.[32] Once, when a stranger showed up at Herrick's apartment and was asked to leave by Herrick's roommate, the stranger refused and lunged and wrestled with the roommate.[33] On another occasion, a man showed up at Herrick's place of work expecting to have sex, and upon hearing that Herrick's profile was an impersonation, began screaming various vulgarities and obscenities at Herrick in front of "all the staff, management, and guests . . . ."[34]

Between November 2016 and January 2017, Herrick reported the fake accounts to Grindr around 50 times.[35] Between January 27, 2017 through March 2017, the fake accounts were reported another 50 times by Herrick, his counsel, or visitors on the site.[36] Grindr has not directly responded to Herrick's reports and have only sent automated replies that say "[t]hank you for your report."[37] Additionally, due to Grindr's silence on the matter, Herrick also filed "approximately 14 police reports and petitioned in Family Court for an order of protection [against JC] to stop the impersonation."[38] In November 2016, he received an Order of Protection against JC, which JC repeatedly violated.[39] Additionally, despite Herrick's multiple reports to the authorities, JC still did not stop.[40]

Herrick v. Grindr was originally filed in New York State Supreme Court,[41] where Justice Kathryn E. Freed issued an ex parte preliminary injunction and a temporary restraining order ("TRO") against Grindr, compelling them to "immediately disable all impersonating profiles created under [Herrick's] name or with identifying information related to [Herrick, Herrick's] photograph, address, phone number, email account or place of work, including but not limited to all impersonating accounts under the

32. *Id.* at 13. ("[B]etween January 13, 2017 and January 17, 2017, 4 to 13 men showed up as Plaintiff's place of employment every single day under the pretense that Plaintiff was going to have sex with them in the bathroom. . . . [And] 13 men visited Plaintiff's home and job expecting to have sex with him.").

33. *Id.*

34. *Id.*

35. Pl.'s First Am. Compl. at 18, *Herrick*, No. 150903/2017.

36. *Id.*

37. *Id.* at 19.

38. *Id.*

39. Brief for Sanctuary for Families, Inc. et al. as Amici Curiae Supporting Plaintiff-Appellant at 8, Herrick v. Grindr, 306 F. Supp. 3d 579 (S.D.N.Y. 2018) [hereinafter *Sanctuary for Families Amicus Brief*].

40. *Id.* Herrick was ultimately arrested on October 23, 2017 and charged with "stalking, criminal impersonation, making a false police report, and disobeying a court order." Tyler Kingkade & Davey Alba, *A Man Sent 1,000 Men Expecting Sex and Drugs to His Ex-Boyfriend Using Grindr, A Lawsuit Says*, BUZZFEED NEWS (Jan. 10, 2019), https://www.buzzfeednews.com/article/tylerkingkade/grindr-herrick-lawsuit-230-online-stalking [https://perma.cc/K33F-N48A].

41. *See Herrick*, No. 150903/2017.

control [of JC]."[42] This TRO expired as a matter of law on February 22, 2017, due to the case's removal to federal court.[43]

On that date, Judge Valerie E. Caproni, of the United States District Court for the Southern District of New York, heard arguments for extending the TRO but ultimately denied the extension.[44] Judge Caproni found that Herrick had not adequately shown that "'extreme or very serious damage' will flow from denial of [the] injunction."[45] Additionally, Judge Caproni's order stated that previous cases "suggest strongly" that Herrick's attempt to separate Grindr's actions from the protections of CDA 230 was a "losing proposition," and thus Herrick's likelihood of success on the merits was low.[46]

Specifically, the type of injunctive relief sought was a TRO to impose an affirmative duty on Grindr to monitor and delete the fake profiles bearing Herrick's name.[47] In the Second Circuit, the standard for granting a TRO resembles that of granting a preliminary injunction.[48] Those standards require that the party seeking a TRO "demonstrate '(1) irreparable harm in the absence of the [TRO] and (2) either (a) a likelihood of success on the merits or (b) sufficiently serious questions going to the merits to make them a fair grounds for litigation and a balance of hardships tipping decidedly in the movant's favor.'"[49]

In denying the extension of the TRO, the court stated that Herrick had not shown the presence of "sufficiently serious questions going to the merits to make the 'fair grounds' for litigation" and did not want to enter into a situation where the court would possibly be engaging in the "day-to-day supervision of Grindr's compliance."[50] Had the court not denied the extension of the TRO, Grindr would have been given a duty that currently does not exist

42. Order to Show Cause for Ex Parte Relief and Temporary Restraining Order, Complaint, Affirmation and Affidavit in Support of Order to Show Cause at 2, *Herrick*, No. 150903/2017.

43. Pl.'s First Am. Compl. at 19, *Herrick*, No. 150903/2017. Additionally, Herrick claims that Grindr violated the TRO, as "there was no change in the number of unwanted visitors" and men still visited him, expecting to have sex with him. *Id.* at 20.

44. First Mot. for Extension of Time, Herrick v. Grindr, 17-CV-932 (VEC), 2017 WL 744605 (S.D.N.Y. Feb. 24, 2017); *Herrick*, 17-CV-932 (VEC), 2017 WL 744605 at *6.

45. Op. and Order at 4, *Herrick*, 17-CV-932 (VEC), 2017 WL 744605 ((*citing* Somoza v. N.Y. City Dep't of Educ., No. 06-CV-5025 (VM), 2006 WL 1981758, at *4 (S.D.N.Y. July 10, 2006) (quoting Phillip v. Fairfield Univ., 118 F.3d 131, 133 (3d Cir. 1997)).

46. *Id.* at 5.

47. *Herrick*, 17-CV-932 (VEC), 2017 WL 744605 (declining to extend TRO that the New York State Supreme Court previously granted).

48. *Id.* at 2 (quoting Andino v. Fischer, 555 F. Supp. 2d 418, 419 (S.D.N.Y. 2008)).

49. *Id.* (quoting MyWebGrocer, LLC v. Hometown Info., Inc., 375 F.3d 190, 192 (2d Cir. 2004)).

50. *Id.* at 5.

under CDA 230.[51] This responsibility would take the form of an interactive computer service, specifically an edge provider[52] (in this case, Grindr) being legally required to affirmatively monitor content on their app—which is in direct opposition to the immunity that CDA 230 provides.[53] However, this Note will assert that although the granting of a TRO currently conflicts with CDA 230, introducing an exception that CDA 230 immunity is not available in matters of fake dating profiles would allow courts to issue TROs, as the underlying requirements of the claim would change and make it possible that a claimant could prevail. Under this new exception, Herrick would have been able to prevail at the hearing for an extension of the TRO, would have been granted injunctive relief against Grindr, and ultimately would most likely have won his entire case. Instead, the Second Circuit affirmed the ruling of the trial court and, in doing so, made clear that CDA 230's protections extend to cell phone applications ("apps"), thus leaving Herrick without any remedies available to him.[54]

III. HISTORICAL BACKGROUND OF THE COMMUNICATIONS DECENCY ACT

In 1996, Congress enacted CDA 230 to help foster the expansion of the Internet as a platform for diverse viewpoints and to expand the interconnectivity of news and information.[55] CDA 230 was promulgated in response to two cases that ruled in inconsistent manners with regard to interactive computer services hosting defamatory content on their site.[56] The

51. *See* 47 U.S.C. § 230 (2018). Currently, CDA 230 does not make providers of interactive computer services liable for "any action voluntarily taken in good faith to restrict access to or availability of material" on their platform. *Id.* Thus, the statute does not impose a responsibility or duty for interactive computer services to monitor the content on their site and similarly does not hold them liable if they chose to take part in any such monitoring. *Id.* An exception does exist in regard to websites that knowingly facilitate sex trafficking. *See* Allow States and Victims to Fight Online Sex Trafficking Act of 2017, H.R. 1865, 115th Cong. (2018); *see also* 47 U.S.C. § 230 (5) (2018).

52. Edge providers "like Netflix, Google, and Amazon, 'provide content, services, and applications over the [I]nternet.'" United States Telecom Association v. Federal Communications Commission, 825 F. 3d 674, 690 (D.C. Cir. 2016) (quoting In re Preserving the Open Internet, 25 FCC Rcd. 17,905, 17, 910 ¶ 13 (2010)).

53. *See* 47 U.S.C. § 230 (c)(2) (2018) ("No provider or user of an interactive computer service shall be held liable on account of … any action voluntarily taken in good faith to restrict access to or availability of material … .).

54. *See generally* Herrick v. Grindr LLC, No. 18-396, 2019 WL 1384092 (2d. Cir. March 27, 2019).

55. *See* 47 U.S.C. § 230(b)(1) (2018); *see also* 47 U.S.C. § 230 (a)(3) (2018) ("The Congress finds . . . [t]he Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.").

56. *CDA 230: Legislative History*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/cda230/legislative-history [https://perma.cc/2LE9-9SVY] (last visited Apr. 9, 2019) [hereinafter *CDA 230: Legislative History*]; *see* Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991); *see also* Stratton Oakmont, Inc. v. Prodigy Services Company, 1995 WL 323710 (Sup. Ct. Nassau County 1995).

first case, *Cubby, Inc. v. CompuServe, Inc.*, involved CompuServe, an "on-line general information service" that, for a membership fee, allowed users to access thousands of sources available on the platform or subscribe to "special interest 'forums'" that host "bulletin boards, interactive online conferences, and topical databases."[57] At issue in this case was the "Journalism Forum" ("Forum") which was an entity independent of CompuServe hired to "manage, review, create, delete, edit and otherwise control the contents" of the Forum.[58] Rumorville USA ("Rumorville") was a publication available as a part of the Forum, and plaintiffs claimed that Rumorville published defamatory content as related to their company.[59] CompuServe did not dispute that the statements were defamatory, but instead argued that, because they were only the distributor and not the original publisher of the content, they couldn't be held liable for the statements.[60]

In ruling that CompuServe was not liable for the defamatory statements, the court analogized CompuServe to a public library, bookstore, or newsstand and stated that, as such, they have "no more editorial control over such a publication" than those entities do over the material they distribute.[61] Further, the court emphasized that the same standard that applies to "more traditional news vendor[s]" needs to apply to a "computerized database" as well, as anything different would thwart the "free flow of information."[62] Finally, the court stated that CompuServe could not be held liable for the defamatory statements if it did not know or had no reason to know of the alleged defamatory statements that were being published.[63] As such, summary judgement in favor of CompuServe was granted.[64]

A few years later, a case with a similar factual background was decided in a different way. In *Stratton Oakmont, Inc. v. Prodigy Services Company*, the plaintiff successfully won their defamation case against Prodigy computer network.[65] Prodigy, an online computer service, provided online computer bulletin boards where users could post and leave comments.[66] At the time of the case, Prodigy's network had "at least two million subscribers" who used the bulletin boards to talk and communicate.[67] The bulletin board at issue in this case, "Money Talk," was "allegedly the leading and most widely read

57. *Cubby, Inc.*, 776 F. Supp. at 137 (S.D.N.Y. 1991).
58. *Id.*
59. *Id.* at 137-38.
60. *Id.* at 138.
61. *Id.* at 139-40. The court also drew on various First Amendment principles, stating that for a distributor to have a duty to "monitor each issue of every periodical it distributes" would pose an "impermissible burden on the First Amendment." *Id.* (citing Daniel v. Dow Jones & Co., 137 Misc. 2d 94, 102, 520 N.Y.S. 2d 334, 340 (N.Y. Civ. Ct. 1987)).
62. *Id.* at 140.
63. *Id.* at 140-41.
64. *Id.* at 141.
65. *See* Stratton Oakmont, Inc. v. Prodigy Services Company, 1995 WL 323710 at *7 (Sup. Ct. Nassau County 1995).
66. *Id.* at *1.
67. *Id.*

financial computer bulletin board in the United States."[68] Plaintiffs alleged that, on Money Talk, an "unidentified bulletin board user" posted defamatory statements about their securities investment banking firm, Stratton Oakmont, saying the firm committed "criminal and fraudulent acts" and that they were "a cult of brokers who either lie for a living or get fired."[69] Stratton Oakmont sued Prodigy for defamation based on the comments posted on the bulletin board, stating that Prodigy was a publisher of the statements and should be held liable.[70]

A significant divergence in the facts of these two cases was that Prodigy expressly held itself out as exercising editorial control over the content of the messages posted on the bulletin boards.[71] The plaintiffs used Prodigy's "software screening program,"[72] "emergency delete function,"[73] and promulgation of "content guidelines"[74] as evidence that Prodigy was in fact a publisher and could therefore be subject to liability in the defamation claim.[75]

The court distinguished a "distributor, or deliverer of defamatory material" from a newspaper, stating that the latter was "more than a passive receptacle or conduit for news, comment and advertising," and said the pertinent question was whether Prodigy "exercised sufficient editorial control over its computer bulletin boards to render it a publisher" that essentially made it more akin to a newspaper than merely a distributor.[76] The court ruled that because Prodigy made decisions as to the content posted on their boards, this constituted "editorial control" rendering them a publisher.[77] Stratton Oakmont won their case against Prodigy and the court's decision turned on Prodigy's active role in moderating the content on their boards—as that made

68. *Id.*
69. *Id.*
70. *Id.* at *2.
71. *Id.*
72. Prodigy's screening program "automatically prescreen[ed] all bulletin board postings for offensive language." *Id.*
73. A function allowing a Board Leader to "remove a note and send a previously prepared message of explanation," as to the reason of removal. *Id.* at *3. The options ranged from "solicitation, bad advice, insulting, wrong topic, off topic, bad taste" and more. *Id.*
74. These guidelines requested that users not post notes "that are 'insulting'" and advised users that "'notes that harass other members or are deemed to be in bad taste or grossly repugnant to community standards, or are deemed harmful to maintain a harmonious online community" will be removed. *Id.* at *2.
75. *Id.* at *5-7.
76. *Id.* at *3.
77. *Id.* at *4. The court also stated that through Prodigy's editorial staff "continually monitor[ing] incoming transmissions," censoring posts, and implementing certain policies and staffing decisions, the company opened itself up to more liability than CompuServe did in *Cubby, Inc. v. CompuServe Inc.* through "gain[ing] the benefits of editorial control." *Id.* at *5.

them a publisher.[78] These two conflicting cases became the impetus for the original passing of CDA 230 in 1996.[79]

When CDA 230 was passed, the courts interpreted the "no liability" component as creating a bar against claims for injunctive relief.[80] The court in *Medytox Solutions, Inc. v. Investorshub.com, Inc*. determined CDA 230 was clear about its constraints based on the text of the statute and that the immunity clearly includes "claims for declaratory and injunctive relief sought."[81] Recently, in *Hassell v. Bird,* the court reaffirmed this position, pointing out that for "almost two decades" courts have been using CDA 230 to preclude injunctive relief when plaintiffs are seeking to hold an interactive content provider as the original publisher of third party content.[82]

Most cases that are successfully dismissed by using CDA 230 as a defense are related to defamation claims.[83] For example, in *Craft Beer Stellar, LLC., v. Glassdoor, Inc.*, the court found that Glassdoor was not liable for the defamatory statements posted on their website, citing CDA 230 as barring Craft Beer Stellar's claim.[84] The court held that although Glassdoor monitored comments in accordance with their community guidelines standards, they didn't "create[] or develop[] the offending information" and thus could not be responsible for them, as they were held to be an interactive content provider.[85]

---

78. *Id.* at *4.

79. *See* Alina Selyukh, *Section 230: A Key Legal Shield For Facebook, Google Is About To Change*, NPR (March 21, 2018), https://www.npr.org/sections/alltechconsidered/2018/03/21/591622450/section-230-a-key-legal-shield-for-facebook-google-is-about-to-change [https://perma.cc/SNH9-67J4]. In 1995, Representative Chris Cox learned of the *Stratton Oakmont* ruling and thought it was "exactly the wrong result" that websites were going to be held liable for the content on their website if they've played an active role in monitoring their platform. *Id.* Cox, along with Senator Ron Wyden, drafted CDA 230, stating "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." *Id.* (quoting 47 U.S.C. §230 (2018)). *See also* 141 Cong. Rec. H8460-01 Aug. 4, 1995.

80. *See Medytox Solutions, Inc. v. Investorshub.com, Inc.*, 152 So.3d 727, 729-31 (Fla. Dist. Ct. App. 2014). The court, in dismissing the plaintiffs' claim for injunctive relief, followed the reasoning of a Third District case stating "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." *Id.* (citing 47 U.S.C. § 230(e)(3) (2018)); *see also* Giordano v. Romeo, 76 So. 3d 1100 (Fla. 3d DCA 2011).

81. *Medytox Solutions, Inc.*, 152 So.3d at 731.

82. Hassell v. Bird, 430 P.3d 776, 793 (Cal. 2018).

83. David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 452 (2010) ("Defamation-type claims were far and away the most numerous claims in the section 230 case law, and the courts consistently held that these claims fell within [S]ection 230's protections.") (citations omitted); *see also* Barnes v. Yahoo!., 570 F. 3d 1096, 1101 (9th Cir. 2009) ("The cause of action more frequently associated with the cases on section 230 is defamation.").

84. Craft Beer Stellar, LLC., v. Glassdoor, Inc., No. 18-10510-FDS, 2018 WL 5505247 at *3 (D. Mass. Oct. 17, 2018).

85. *Id.*

Similarly, in *Igbonwa v. Facebook, Inc.*, Igbonwa filed a claim against Facebook for defamation based on comments posted on the social media platform.[86] The plaintiff was attempting to hold Facebook liable for information posted by an "information content provider," and the complaint argued that Facebook was liable as the "publisher or speaker" of that information—clearly falling within CDA 230's scope.[87] However, Facebook contended, and the court agreed, that they were immune from liability because they were an interactive computer service.[88]

IV. CDA 230'S APPLICATION IN CASES REGARDING FAKE PROFILES

CDA 230 protects interactive computer services against other claims, in addition to libel and defamation claims.[89] Specifically, interactive computer services have recently and successfully claimed immunity against plaintiffs seeking to hold them liable for fake profiles hosted on their sites[90]—for example, via a breach of contract for violations of terms of service theory.[91]

In *Barnes v. Yahoo!, Inc.*, Barnes' ex-boyfriend created profiles of her on a website run by Yahoo!.[92] Barnes got calls, emails, and personal visits by individuals expecting sex based on the profile posting.[93] Per Yahoo!'s policy, Barnes sent a copy of her photo ID and "a signed statement denying her involvement with the profiles and requesting their removal," but no response or action came of it.[94] During this time, a "local news program was preparing

86. Igbonwa v. Facebook, Inc., No. 18-cv-02027-JCS, 2018 WL 4907632 at *1 (N.D. Cal. Oct. 09, 2018).

87. *Id.* at *5 (quoting Klayman v. Zuckerberg, 753 F.3d 1354, 1357 (D.C. Cir. 2014) (citing 47 U.S.C. § 230(c)(1) (2018))).

88. *See id.*

89. *See generally* Ardia, *supra* note 83, at 427-29.

90. *See, e.g.*, Dehen v. DOES 1-100, No. 17-cv-198-LAB, 2018 WL 4502336 (S.D. Cal. Oct. 19, 2018) (regarding fake Twitter accounts); *see also* Carafano v. Metrosplash.com Inc., 339 F. 3d 1119 (9th Cir. 2003). In *Carafano,* the Ninth Circuit stated that Matchmaker.com was immunized under CDA 230 for a fake profile that was uploaded of actress Christianne Carafano. *See Carafano*, 339 F. 3d at 1121. The fact that some of the content uploaded was in response to the website's questionnaire did not alter the court's decision nor make the website an information content provider, as the court reasoned that "no profile has any content until a user actively creates it." *Id.* at 1124. The court did not discuss the possibility of injunctive relief as the suit was filed after Matchmaker.com removed the profile from their website. *See id.* at 1122.

91. *Dehen*, No. 17-cv-198-LAB, 2018 WL 4502336 at *4-5 (claiming that due to Twitter's failure to remove the fake profiles they were in violation of their terms of service and thus breaching the contract they entered with Dehen when she registered for their service).

92. Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1098 (9th Cir. 2009). The profiles were posted without Barnes' permission, contained indecent content and were "some kind of solicitation . . . to engage in sexual intercourse." *Id.* The online profiles also contained Barnes' personal information, such as her addresses, both physical and electronic, and her work phone number. *Id.*

93. *Id.*

94. *Id.* Barnes contacted Yahoo! two more times the following month. *Id.*

to broadcast a report on the incident[,]" and one day before this broadcast, Yahoo!'s Director of Communications told Barnes she would directly hand Barnes' statement to the correct division and that it would be handled.[95] However, when two months passed and nothing had changed, Barnes filed suit in Oregon state court, and shortly after, the profiles disappeared and never returned.[96] The court dismissed Barnes' claims, stating that CDA 230 immunized Yahoo!,[97] but allowed the promissory estoppel claims to move forward, as CDA 230 doesn't bar breach of contract suits.[98]

Similarly, in *Dehen v. DOES 1-100*, Dehen sued Twitter in response to fake accounts that were opened in her name in an effort to impersonate and defame her.[99] Twitter was successfully immunized under CDA 230 as they met the requirements to be classified as an interactive computer service; they were being treated as a "publisher" or "speaker" of the content and the content was in fact "provided by another information content provider."[100] Thus, Twitter was shielded from liability by the statute and immunized from the claims against them.[101]

With these cases, courts have been clear that CDA 230 covers interactive content providers against suits relating to fake profiles on their sites.[102] However, some courts have been less consistent when it comes to the possibility of obtaining injunctive relief when CDA 230 is invoked to immunize an interactive content provider.[103]

---

95. *Id.* at 1099. Barnes, relying on this statement, took no further action on her own. *Id.*

96. *Id.*

97. *Id.* at 1105-06. The court did not discuss the availability of injunctive relief in this case. *See generally Barnes*, 570 F.3d 1096.

98. *Barnes*, 570 F.3d at 1109. The court explained that while CDA 230 has a "baseline" rule of no liability for information service providers, when the court concludes that a promise is legally enforceable under contract law, it has concluded that the "promisor has manifestly intended that the court enforce his promise." *Id.* This then removes it from CDA 230 protection and frames it into a breach of contract theory where the provider can be found liable, as they were here. *Id.*

99. Dehen v. DOES 1-100, No. 17-cv-198-LAB, 2018 WL 4502336 at *1 (S.D. Cal. Oct. 19, 2018).

100. *Id.* at *3. The requirements being: (1) the entity being sued provides an "interactive computer service" (2) plaintiff's claim treats the defendant as the "publisher" or "speaker" of the offending content, and (3) the content was "provided by another information content provider." *Id.* (quoting *Barnes*, 570 F. 3d at 1100-01).

101. *Id.* at *4.

102. *See generally Dehen*, No. 17-cv-198-LAB< 2018 WL 4502336; *see also Barnes*, 570 F. 3d at 1100-01.

103. *See* Smith v. Intercosmos Media Group, Inc., No. Civ. A.02-1964, 2002 WL 31844907 at *4 (E.D. La. 2002) ("[C]laims made by the plaintiffs for damages or injunctive relief . . . are precluded by the immunity afforded by Section 230(c)(1)."). *But see* Mainstream Loudoun v. Board of Trustees of Loudoun County Library, 24 F. Supp. 2d 552 (E.D. Va. 1998) (allowing for injunctive relief under CDA 230).

V. INCONSISTENCY IN THE AVAILABILITY OF INJUNCTIVE RELIEF UNDER CDA 230

Courts have differed on how to rule on the viability of injunctive relief when CDA 230 provides immunity to a defendant from damages.[104] In some instances, courts have ruled that CDA 230 does not immunize a defendant against a claim that is seeking declaratory and injunctive relief.[105] The courts in these cases reasoned that if Congress wanted the statute to immunize providers against "both liability and declaratory and injunctive relief," it would have written it into the statute.[106]

However, other courts have determined that CDA 230's immunity clearly encompasses injunctive relief, and that the statute's "no liability" provision bars other types of relief in addition to damages.[107] Courts have concluded that sometimes injunctive relief is "at least as burdensome" as damages and "typically more intrusive"—reasoning that if the stated purpose of CDA 230 is to immunize interactive computer services for statements made by third parties, then making them legally responsible for the content also defeats that purpose.[108]

The cases in which courts have explicitly expressed a view on the availability of injunctive relief—one way or another—have not been cases regarding fake profiles, fraud, or impersonation.[109] With courts split on the matter,[110] there is an opening in CDA 230 and injunctive relief jurisprudence to allow for an exception that would introduce a new standard of proof in order to be able to successfully claim CDA 230 immunity in cases of fraud

104. *See* Morrison v. American Online, Inc., 153 F. Supp. 2d 930, 934-35 (N.D. Ind. L.R. 2001) ("A review of the various cases addressing whether the statutory immunity of Section 230 applies to injunctive relief reveals a disagreement among various courts.").

105. *See Mainstream Loudoun*, 24 F. Supp. 2d at 561.

106. *See id.*; *see also* Does v. Franco Productions, No. 99 C 7885, 2000 WL 816779 (N.D. Ill. June 22, 2000) ("Plaintiffs' claims for injunctive relief, although not precluded by the CDA, fail to state a claim.").

107. *See* Kathleen R. v. City of Livermore, 87 Cal. App. Rptr. 2d 772, 781 (Ct. App. Cal. March 6, 2001). The court also found its interpretation consistent with a previous Tenth Circuit case which concluded injunctive relief was barred under CDA 230 immunity. *Id.* (citing Ben Ezra, Weinstein, & Co. v. America Online Inc., 206 F. 3d 980, 983-84 (10th Cir. 2000)).

108. *See* Noah v. AOL Time Warner, Inc., 261 F. Supp. 2d 532, 540 (E.D. Va. 2003).

109. *See, e.g.*, Smith v. Intercosmos Media Group, Inc., No. Civ. A.02-1964, 2002 WL 31844907 (E.D. La. 2002); *Mainstream Loudoun*, 24 F. Supp. 2d at 561; *Morrison*, 153 F. Supp. 2d at 934-35.

110. *See Smith*, No. Civ. A.02-1964, 2002 WL 31844907 at *4-5 (stating that injunctive relief is precluded under CDA 230). *But see Mainstream Loudoun*, 24 F. Supp. 2d at 561 (allowing for injunctive relief under CDA 230).

and impersonation online.[111] This would likely increase the likelihood of a plaintiff's ability to succeed on the merits of their claim—thus increasing the likelihood of the availability of being granted injunctive relief. This proposal has some basis in modern legal decisions, seeing that in 2017 the New York State Supreme Court granted Herrick injunctive relief against Grindr, deeming that it was a viable option in the face of CDA 230 immunity.[112]

The availability of injunctive relief in cases pertaining to fake profiles and impersonation should be viewed inherently differently than when injunctive relief is sought in matters concerning defamatory comments and libelous statements. Impersonation and fake profiles are actions commonly done by abusive partners in an effort to "exploit, harass, threaten, and stalk their victims."[113] This type of abuse comes in the form of "nonconsensual disclosure" when images, videos, and personal information are published online for other users to use in order to "stalk, harass, or assault" the victim.[114] The abuse Herrick experienced "is among the most accessible forms of abuse available," as all that is needed to employ this harassment and abuse is the Internet.[115] This leaves victims helpless, and without the ability to receive relief from the courts against the platforms that are hosting these fake profiles, or the dating apps that are perpetuating their use, they are left suffering from this cyber harassment—just as Herrick is, years later.[116] This Note's proposal has two sources of justification that lend support to an exception within CDA 230: Congress' original intent is not at odds with this proposed exception and the underlying tenants of another exception, the Fight Online Sex Trafficking Act[117] and Stop Enabling Sex Traffickers Act,[118] would lend support.

---

111. Some have proposed that actual liability be attached to interactive computer services, under a theory of distributor liability, akin to what was seen in FOSTA-SESTA. *See* Colleen M. Koch, *To Catch a Catfish: A Statutory Solution for Victims of Online Impersonation*, 88 U. COLO. L. REV. 233, 273 (2017). However, this proposal does not go as far, for it is not proposing that liability be attached if interactive computer services "know or should have known[,]" but would instead allow for an avenue for the courts to compel these services to delete the fake profiles when the victim brings a successful suit against them. *Id.*

112. Order to Show Cause for Ex Parte Relief and Temporary Restraining Order, Complaint, Affirmation and Affidavit in Support of Order to Show Cause at 1-2, Herrick v. Grindr, No. 150903/2017 (N.Y. Sup. App. Div., Jan. 27, 2017).

113. *Sanctuary for Families Amicus Brief*, *supra* note 39, at 9.

114. *Id.* at 10.

115. *Id.* at 15. *See also* Monica Anderson, *Key takeaways on how Americans view – and experience – online harassment,* PEW RESEARCH CENTER (July 11, 2017), http://www.pewresearch.org/fact-tank/2017/07/11/key-takeaways-online-harassment/ [https://perma.cc/8DZ6-X9JK] ("Nearly nine-in-ten Americans (89%) say the ability to post anonymously enables people to be cruel or harass one another.").

116. *See generally* Pl.'s Compl. 3-16, 23-25.

117. H.R. 1865, 115th Con. (2018). Hereinafter "FOSTA."

118. S. 1693, 115th Cong. (2018). Hereinafter "SESTA."

A. Congress Did Not Enact CDA 230 with Fraud or Impersonation in Mind

When Congress passed CDA 230, it was in response to two defamation cases,[119] and as such, was often viewed as providing protection for interactive computer services against libel claims.[120] In fact, from the statute's enactment in 1996 to 2009, 50.5% of the legal claims that utilized a CDA 230 defense were for "defamation, libel, slander, and disparagement . . . ."[121] Congress' stated intent with passing CDA 230 was to "promote the free exchange of information and ideas over the Internet and to encourage voluntary monitoring for offensive or obscene material."[122] This intent, paired with the vast number of defamation claims in which CDA 230 immunity is invoked,[123] goes to show that this Note's proposed exception would likely not be at odds with the vast amount of the litigation pleadings—as it would be creating a carve out exception that doesn't affect defamation claims.

Fake news, profiles, and impersonation accounts online are not seen as aiding in the spread of valuable information in the marketplace of ideas, or even as a beneficial addition to the exchange of information online.[124] Thus, one could argue that allowing fake profiles and impersonation accounts to remain online, with no relief for victims, would be directly against Congress' intent and thus does not fit within CDA 230's rationale. The contours of the specific requirements will be covered further in Section VI, but it is important to note that the proposed exception contains a malicious intent requirement as well as an inducement requirement—thus harmless parody accounts would not be within its purview. These harmless parody accounts, as they are a protected type of speech under the First Amendment,[125] would be a category of speech that this proposed exception would work to avoid removing.

---

119. *CDA 230: Legislative History, supra* note 56. *See also* Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991); Stratton Oakmont, Inc. v. Prodigy Services Company, 1995 WL 323710 (Sup. Ct. Nassau County 1995).

120. As CDA 230 expressly overruled *Stratton Oakmont*, a case that imposed liability on an Internet provider for content on their website, it makes sense to view libel and defamation cases as the types of cases against which Congress wanted to protect Internet providers. *See* H.R. Conf. Rep. No. 104-458, at 194 (1996).

121. Ardia, *supra* note 83, at 429-30.

122. Joseph Monaghan, Comment, *Social Networking Websites' Liability for User Illegality*, 21 SETON HALL J. SPORTS ENT. L. 499, 504 (2011).

123. *See* Ardia, *supra* note 83, at 430.

124. *See generally* Renee Diresta, *Free Speech In The Age of Algorithmic Megaphones*, WIRED (Oct. 12, 2018, 4:19 PM), https://www.wired.com/story/facebook-domestic-disinformation-algorithmic-megaphones/ [https://perma.cc/HJT5-YJDM] ("When viewed holistically, these manipulative activities call into question the capacity of social media to serve as a true marketplace of ideas—and this is not a new concern."); *see also* Philip M. Napoli, *What If More Speech Is No Longer the Solution? First Amendment Theory Meets Fake News and the Filter Bubble*, 70 FED. COMM. L.J 55, 88 (2018) ("The irony here is that fake news is a type of speech that is most directly and irrefutably damaging to the integrity of the democratic process.").

125. *See* Hustler v. Falwell, 485 U.S. 46, 46-47 (1988).

B. The Reasoning Behind the Exception Would Be Akin to the Reasons that FOSTA-SESTA Was Passed

When FOSTA-SESTA was signed into law by President Trump in 2018,[126] the bill created a significant exception to CDA 230 immunity by clarifying that the statute does not protect interactive computer services from laws relating to "sexual exploitation of children or sex trafficking."[127] These bills also hold these services liable and responsible if third parties are posting information relating to sex-trafficking or prostitution on their site.[128] Most notably, these bills place an affirmative duty on providers to monitor content on their website and completely place the "onus on website owners to self-police,"[129] as FOSTA can be used as the basis for civil action against a website found to be "knowingly assisting, supporting, or facilitating a sex trafficking violation"[130] or "advertisements for sex work."[131]

The bottom-line effect of FOSTA and SESTA—punishing and holding publishers liable for hosting information about sex trafficking and prostitution[132]—can be readily applied here. When passed, FOSTA-SESTA was said to "ensure that victims and survivors of sex trafficking can seek justice against websites that knowingly facilitated the crimes against them."[133] Senators in support of the bill recognized that it would strike a balance between holding sex traffickers accountable and "allowing free speech and innovation to continue to thrive."[134] Importantly, the bills are meant to protect vulnerable groups and communities from the bad actors that exploit them.[135] The bills give these groups the "legal tools needed to seek and receive justice from all those involved" by no longer allowing these providers to have the blanket protection that CDA 230 can provide.[136]

However, these bills have endured extreme criticism—perhaps rightfully so—about the detrimental effects they have in practice for sex

126. Tom Jackman, *Trump signs 'FOSTA' bill targeting online sex trafficking, enables states and victims to pursue websites*, WASH. POST (Apr. 11, 2018), https://www.washingtonpost.com/news/true-crime/wp/2018/04/11/trump-signs-fosta-bill-targeting-online-sex-trafficking-enables-states-and-victims-to-pursue-websites/?utm_term=.c419a71015dd [https://perma.cc/77FE-3FGT].

127. 164 Cong. Rec. H.R. 1731, 1865 (March 21, 2018).

128. *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), https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom **[**https://perma.cc/JCS8-EJPB] (last visited Apr. 9, 2019) (explaining that FOSTA-SESTA meant to "curb sex trafficking on online personal sites").

129. *Id.*

130. H.R. 1865, 115th Con. § 5 (2018).

131. Romano, *supra* note 128.

132. *See* H.R. 1865, 115th Con. § 5 (2018).

133. 164 Cong. Rec. H.R. 1865 (March 21, 2018).

134. *Id.* (statement of Sen. Schumer).

135. *See* Romano, *supra* note 128.

136. 164 Cong. Rec. S.R. 1731, 1859 (March 21, 2018).

workers and prostitutes.[137] Opponents of the bill cite studies purporting to show that online communications make "sex work safer"—for example, a 2017 study showed a "17 percent decrease in homicide of female victims after Craigslist erotic services were introduced in various cities."[138] They also point to the direct impact these laws have had on sex workers' ability to research and screen clients, report dangerous situations to other workers, and share important and possibly dangerous health information about clients to the community at large.[139] Without access to these forums, sex workers are forced to go on the streets without being equipped with crucial information, and are more susceptible to "violence, STIs, and exploitation"—putting their health and safety directly at risk.[140]

FOSTA and SESTA hold providers accountable for "knowingly assisting, supporting or facilitating a violation,"[141] and do not take a provider's intent or motives into account. Further, it may not be evident if the content is for consensual sex work or sex trafficking—thus many websites take "action to censor or ban parts of their platforms" because discerning which ads are promoting consensual versus nonconsensual sex is too difficult.[142] This Note's proposed exception would require both a showing of malicious intent and a showing of inducement by the individual that created the fake profiles. These requirements, which FOSTA-SESTA lacks, will likely not overly burden speech by sweeping too broadly. For example, they won't affect parody accounts that aren't aimed to harm anyone. Further, these requirements would make sure the speech being removed from these platforms is not serving a justifiable purpose and would thus limit any unintended consequences that can occur from flat bans that stem from the strict liability seen in FOSTA-SESTA cases.[143] This distinction is important because currently in FOSTA-SESTA, advertisements can be taken down regardless of whether the intent or goal of the person who posted it is for illegal sex trafficking or consensual sex work.[144] In this Note's proposal, the intent requirement ensures that the motivations behind the fake accounts are taken into account.

---

137. *See* Siouxsie Q, *Anti-Sex-Trafficking Advocates Say New Law Cripples Efforts to Save Victims*, ROLLING STONE (May 25, 2018, 7:01 PM), https://www.rollingstone.com/culture/culture-features/anti-sex-trafficking-advocates-say-new-law-cripples-efforts-to-save-victims-629081/ [https://perma.cc/P995-GPZQ].

138. Briana Hauser, *FOSTA/SESTA Becomes Law Despite Strong Opposition*, GEO. L. TECH. REV. (LEGAL NEWS) (2018), https://georgetownlawtechreview.org/fostasesta-becomes-law-despite-strong-opposition/GLTR-04-2018/ [https://perma.cc/B4ER-7RN9].

139. *Id.*

140. *Id.*

141. H.R. 1865, 115th Cong. § 5 (2018).

142. Romano, *supra* note 128.

143. *See* Tina Horn, *How a New Senate Bill Will Screw Over Sex Workers*, ROLLING STONE (Mar. 23, 2018), https://www.rollingstone.com/politics/politics-features/how-a-new-senate-bill-will-screw-over-sex-workers-205311/ [https://perma.cc/L9A4-JNX9] ("When platforms over-censor their users, marginalized communities are often silenced disproportionately.").

144. *Id.* ("The threat of prosecution has already led such forums to simply shut down rather than face potential legal liability.").

Comparable to the balance between accountability and free speech ideals that a majority of Congress found was met in FOSTA-SESTA, creating an exception by changing the underlying provisions of CDA 230 for fraud and impersonation cases and in effect allowing injunctive relief for victims of these cases could do the same thing. As will be discussed in Section VI, apps and interactive computer services (specifically, edge providers) can implement identity verification steps to make sure the profiles taken down are in fact fake ones.

Finally, cyber abuse and harassment is a troubling issue in American society, with about four-in-ten Americans personally experiencing a form of online harassment.[145] Even more troubling is that "certain groups are more likely than others" to experience trait-based harassment, creating vulnerable communities and groups of people that are in desperate need of recourses.[146] The availability of injunctive relief would hold these providers responsible for answering and addressing victim concerns and impose an affirmative duty (should a court issue the injunctive relief), that a majority of the population[147] believes they should be responsible for. These statistics reflect the pervasiveness of cyber harassment and abuse that justifies imposing liability on providers in the same way that a majority of Congress believed that passing FOSTA-SESTA was justified in order to hold providers responsible for hosting content facilitating sex trafficking.

VI. INTRODUCING AN EXCEPTION TO CDA 230

Introducing injunctive relief as an option in cases where a provider is no longer technically immune (after this Note's proposed congressional amendment to CDA 230 is passed), would still require the plaintiff to adhere to a specific process and a different standard of proof in order to get relief. The provider—be it a dating app or dating website—would still not have to actively monitor for fake profiles, as CDA 230 imposes no affirmative duty to monitor, and this proposal does not suggest that such a duty should be imposed. Specifically, this proposed exception is explicitly intended to address impersonation dating app accounts. The harms posed by such

145. Maeve Duggan, *Online Harassment 2017*, PEW RESEARCH CENTER 1 (July 11, 2017), http://www.pewinternet.org/2017/07/11/online-harassment-2017/ [https://perma.cc/86K6-35S4].

146. *Id.* at 3. According to a 2017 Pew Research Center survey on online harassment, one-in-four blacks and one-in-ten Hispanics have been targets of online harassment due to their race or ethnicity. *Id.*

147. *Id.* at 4 (stating 79% of Americans think that it is the responsibility of the online services to intervene and stop the "harassing behavior [that] occurs on their platform . . . ."); *see also* Jonathan Stempel, *Grindr defeats appeal over harassment on gay dating app*, REUTERS (March 27, 2019), https://www.reuters.com/article/us-grindr-app/grindr-defeats-appeal-over-harassment-on-gay-dating-app-idUSKCN1R81WD [https://perma.cc/Y9R7-M89B] ("What happened to [] [Herrick] is not an isolated incident, . . . [a]pps are being used to stalk, rape and murder. Under the court's reading of the CDA, big tech companies don't have responsibility to do anything about it, even if they know it is happening. Congress needs to amend this statute.").

accounts are uniquely pervasive, as seen in *Herrick v. Grindr,* and necessitate different requirements and their own exception to combat the problem.

Accordingly, a procedure similar to the one henceforth mentioned may be what is necessary to provide recourse for plaintiffs and victims affected by fraud and impersonation on dating apps and to enable them to re-establish the normalcy in their life that has been stripped away.

Successfully prevailing under this specific contort of CDA 230 pertaining to fake profiles and online impersonations would require the following: first, the plaintiff must follow all the adequate procedures set in place (if any exist) with the dating app or website to alert them to the presence of the fake profile.[148] Taking part in this process does not need to be successful or even yield a response from the provider[149]—the plaintiff would only be required to show their good faith attempt to alert the provider to the impersonation before legal recourse is available. Further, a set waiting period would be imposed in order to give the provider time to answer the complaint and possibly resolve the issue before it goes to the courts. One suggestion is a maximum period of two to three weeks.[150]

Second, after the requisite waiting period has passed, and if the fake profile is still live, the plaintiff needs to then satisfy a reasonableness requirement. For this, the burden is on the plaintiff to affirmatively show that their request is a reasonable one. This is a multi-factor test and no factor alone is dispositive—however, when taken into account and based on the totality of the circumstances, a combination of these various factors can help to prove reasonableness on the part of the plaintiff. A showing that the individual seeking recourse is a private figure and not a public one will factor in, as private figures have significantly less means of recourse to clarify and disseminate the truth about them in the face of lies.[151] Additionally, the content being posted can be of importance when looking at the take down request in its totality. For example, in *Herrick v. Grindr*, the content at issue would have been very clearly viewed under this new exception as low value

148. This may very well be the end of the fake profiles and impersonations for the plaintiff. For example, for Herrick, when another "lesser-known gay dating app, Scruff[,]" had Herrick's fake profiles on them, he filed a complaint with them and the company deleted and banned the account within 24 hours. Andy Greenberg, *Spoofed Grindr Accounts Turned One Man's Life Into A "Living Hell,"* WIRED (Jan. 31, 2017 02:57 PM), https://www.wired.com/2017/01/grinder-lawsuit-spoofed-accounts/ [https://perma.cc/E3WX-CLF6]. Scruff also "prevented the same device or IP address from creating any new accounts," taking Herrick's claims seriously and working to help him quickly. *See id.*; *see also* Carafano v. Metrosplash.com Inc., 339 F. 3d 1119 (9th Cir. 2003) (explaining that, after alerting Matchmaker to the fake profiles, the company, upon request, deleted the fake profile before a complaint was filed in California state court).

149. The plaintiff would, however, need to show evidence of successfully adhering to all the procedures that are in place.

150. While this is a relatively short waiting period, any longer might risk significant harm to the plaintiff at the hands of the fake profiles. Thus, to balance the plaintiff's interest in not prolonging cyber abuse and harassment with the provider's interest and realistic capabilities to respond to requests, a period of 2-3 weeks should be a fair middle ground for both parties.

151. *See generally* Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974).

speech, as JC had spread lies about Herrick's very personal sexual life, published Herrick's address and in doing so, placed him in direct harm.[152]

The intent of the individual who is creating the content must also be analyzed and classified. The malicious intent prong would require the plaintiff to prove the individual impersonating him or her was doing it with an intent to harm the plaintiff and created the fake profile to cause that harm.[153] This requirement would ensure that parody accounts, for example, that are created with the goal of comedic relief are not swept up in this exception. The malicious intent in these cases could be aided by a showing of what the content actually is. For example, in Herrick's case, a reasonable person would most likely concur that JC's intent and motivations were malicious, based on the content of the lies he was spreading.[154]

Additionally, realistic intent can also work its way into this analysis. If the matter is between two private citizens and one is mocking the other, more likely than not the intent is malicious and not pure. What further supports this theory is that, if the mocking was lighthearted and with the consent of the one mocked, it most likely wouldn't have found its way into the court system at all.

Further, the plaintiff would be aided in their showing of reasonableness by proving that the fake profile spread false information and induced individuals by reaching out to them and engaging in conversations under the guise of being the plaintiff. Inducing individuals to believe the profile is real and holding the profile out as a real profile, is a very different situation than a fake profile that merely exists but neither seeks to convince others it is something it is not nor actively tries to spread misinformation about someone.

Because these factors are holistic and not determinative, there may be other factors that aid in the formulation of reasonableness. However, by weighing these factors in light of the totality of the circumstances, courts could be better equipped to determine when a dating app can claim that CDA 230 makes them immune and when a plaintiff has successfully shown that his situation should fall under the new exception to CDA 230.

As for the logistics of tangible proof that the profile is in fact fake, a plaintiff could submit copies of their driver's license or other verified forms of identification to prove their identity, as well as copies of the profiles that are impersonating them, a signed affidavit that these profiles were not created with their consent or approval, and, finally, the name of the profiles they want removed if they are successful in their plea for injunctive relief.

Third, if the reasonableness standard is met, and the court believes that the plaintiff is likely to succeed on the merits and thus grants injunctive relief, it would be the plaintiff's responsibility to show the provider exactly which profile(s) are fake and which ones they want taken down, and to give the

---

152. *See generally* Herrick v. Grindr, LLC., 306 F. Supp. 3d 579, 585 (S.D.N.Y. 2018) (quoting Pl.'s Am. Compl. ¶¶ 49-50).

153. *See, e.g.*, New York Times Co. v. Sullivan, 376 U.S. 254, 279-80 (1964) ("'[A]ctual malice—that is, with knowledge that it was false or with reckless disregard of whether it was false or not.'").

154. *See Herrick*, 306 F. Supp. 3d at 585 (quoting Pl.'s Am. Compl. ¶¶ 49-50).

provider the plaintiff's accurate contact information so the provider can have it on file. This accurate contact information would include the plaintiff's email address, phone number, physical address, and a picture. This could help to streamline the process if other fake profiles continue to pop up with the plaintiff's photo, but with different contact information.

Fourth, a successful grant of injunctive relief would place the onus on the plaintiff, rather than the provider, to search the dating apps for any new or additional fake profiles, in order to request subsequent removals. This approach benefits both the plaintiffs and the providers. The plaintiffs, while undertaking the duty to find the fake profiles, can feel comfortable that the exact profiles they are concerned about are getting deleted. The providers can feel secure that their rights and lack of affirmative duty to monitor under CDA 230[155] are not being thwarted, and that little to no economic burden is being imposed on them as they do not have to hire individuals to take on an affirmative role to search and locate fake profiles.[156]

A. Pros, Cons, and Effects of the Proposed Exception

A clear benefit of this exception would be providing individuals with the autonomy to protect and control their online presence. As seen in *Herrick v. Grindr,* an individual currently has no legal recourse when fake dating profiles are created and used to spread false information about him or her and to induce others to believe and rely on those falsities.[157] This was apparent in Herrick's case, for example, as individuals that relied on their conversation with the fake profiles on Grindr showed up to his home and work and engaged in extremely harassing behavior.[158]

A disadvantage of this exception is that it would lead to a degree of judicial interference currently not seen anywhere besides matters falling under FOSTA-SESTA's umbrella. This could create opposition for the same reason those laws did, as the exception would also have the possibility of thwarting free speech rights while also taking away the autonomy that dating apps currently have in deciding how to address issues of impersonation. Additionally, it is unclear if this exception would be successful in limiting the access of individuals who impersonate others online. This limitation would most likely have to be addressed in a dating app company's internal policies and guidelines, giving them discretion as to whether an individual who has

155. *See* 47 U.S.C. § 230 (c)(2) (2018).

156. Herrick's lawyer also acknowledged this. Carrie Goldberg said that providers such as Grindr don't respond to complaints or actively do anything because "[i]t's cheaper for them not to staff a department that addressees complaints and abuses of the product." Greenberg, *supra* note 148. This proposal takes into account Goldberg's statement when it recommends placing the responsibility on the plaintiff to find and flag the fake profiles instead of the provider. *See id.*

157. *See* Herrick v. Grindr, No. 18-396, 2019 WL 1384092, at *2 (2d. Cir. Mar. 27, 2019).

158. Pl.'s Compl. at 12, Herrick v. Grindr, No. 150903/2017 (N.Y. Sup. App. Div., Jan. 27. 2017).

impersonated individuals in the past could legitimately create a profile for themselves on the app in the future.

However, the high bar that is required of the plaintiff works to ensure that only those accounts that are actually causing or will cause harm are being taken down, and thus will not likely result in the over removal of dating app profiles. As with all new proposals and changes of law, there is a possibility that this exception may affect some individuals outside of the intended group at the outset of its application. Because of this, the courts may rightfully modify the factors in the reasonableness test and perhaps place a higher burden on the plaintiff to ensure that no protected speech is being removed. Additionally, lawmakers may choose to embed additional safeguards to the exception in order to prevent it from becoming an overly vague and motive-independent law—to avoid the pitfalls in the way that FOSTA-SESTA was drafted.[159]

As for the punishment for the individuals that create fake dating profiles, courts would need to look at state fraud and impersonation laws to determine the correct civil remedy.[160] That being said, this exception does not encompass or pertain to a joint suit against the dating app and the individual responsible.

VII. CONCLUSION

Under this proposed amendment to CDA 230 allowing for an exception for matters of online fraud and impersonation, a plaintiff is more likely to obtain injunctive relief because they are more likely to be successful on the merits of their underlying claim. Under this proposal, Herrick's injuries and traumas could have ended almost as quickly as they began because he was already equipped with the knowledge that JC was responsible.[161] JC spread false information about Herrick, inducing individuals to show up at Herrick's home and work, which presumably proves JC's malicious intent.[162] With that information and evidence, Herrick would have successfully sought relief from a court adopting this Note's proposed exception and would have gotten the fake dating profiles removed. This would have ended Herrick's emotional and physical suffering at the hands of JC and prevented countless random men from showing up and taunting and harassing him. This exception could have allowed Herrick to get his life back and feel safe again.

This proposal would arm victims with the power they need to take control of fake online personas that paint an inaccurate picture of an

159. Romano, *supra* note 128. (*"*[N]umerous websites took action to censor or ban parts of their platforms in response — not because those parts of the sites actually *were* promoting ads for prostitutes, but because policing them against the outside possibility that they *might* was just too hard.").

160. *See, e.g.*, *Identity Theft*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/financial-services-and-commerce/identity-theft-state-statutes.aspx [https://perma.cc/S4SK-JEN] (last visited Apr. 9, 2019).

161. *See* Herrick v. Grindr, 306 F. Supp. 3d 579, 584 (S.D.N.Y. 2018).

162. *See id.*

individual, at best, and help to perpetuate sexual assault, harassment, and rape at worst. It would create a way for victims of fraud and impersonation via fake dating app profiles to finally seek help within the confines of established CDA 230 immunity and interactive computer services' current lack of affirmative duty to monitor.