LIKE IT OR NOT: RECOGNIZING A SPECIAL RELATIONSHIP BETWEEN SOCIAL MEDIA COMPANIES AND THEIR USERS

*Alexandra Tran**

When the internet plays a role in a plaintiff's injury, there can be considerable roadblocks barring recovery. At the heart of the dispute over how social media should be legally addressed is the balance between maintaining freedom of expression on the open internet and imposing regulations on social media companies to ensure online safety. When plaintiffs allege that a social media company had a duty to warn them about dangers on its site, courts are generally reluctant to extend the special relationship doctrine to encompass the social media-user relationship. In addition to the high bar set by courts, different jurisdictions vary in their analyses of the special relationship question, often resulting in the plaintiffs' claims being dismissed.

This Note examines the different factors that courts consider when deciding whether to create a special relationship, both in internet and noninternet cases. This Note then advocates for courts to place greater emphasis on a social media company's superior knowledge when evaluating the company's duty to warn. To demonstrate how that may affect the outcome of future cases, this Note will analyze Internet Brands v. Doe *from the U.S. Court of Appeals for the Ninth Circuit through the lens of superior knowledge. This Note concludes by recognizing the importance of social media in modern society but ultimately calls for legal reform to hold social media companies responsible for the safety of their users.*

* J.D. Candidate, 2026, Fordham University School of Law; B.A., 2023, University of Virginia. Thank you to Professor Chinmayi Sharma, Alex Wildman, and the editors and staff of the *Fordham Law Review* for their invaluable guidance and feedback. I would also like to thank my family and friends for their love, encouragement, and support throughout this process.

INTRODUCTION

The rise of social media has ushered in an age where a few clicks can lead to love, friendship, or peril. It has revolutionized human interaction, connecting billions of people across the globe and creating unprecedented opportunities to meet, share, and comment. But this connectivity also exposes users to significant dangers, from misinformation and harassment to exploitation and injury. Even the U.S. Supreme Court has recognized that social media platforms wield a double-edged sword, noting that they "make our lives better, and make them worse—create unparalleled opportunities and unprecedented dangers."[1] For example, a 2022 review of dating app–facilitated sexual assault found that sexual assaults committed by someone that the victim met on a dating app, as compared to those committed by

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

someone from outside of a dating app, tended to be more violent.[2] Based on these findings, the researchers proposed that sexual predators may use dating apps to hunt for vulnerable victims.[3] Moreover, another study analyzed social media's involvement in the perpetration of violent crime in Maryland.[4] There, researchers concluded that social media was involved in approximately 1.4 percent of 15,168 violent offenses from 2018 to 2021 in Prince George's County, Maryland.[5] Of these, injury occurred in 71.4 percent of cases in which social media was used to make threats.[6] For victims like Mary Kay Beckman, who was stabbed in her home by a man she met on Match.com ("Match"),[7] these findings are more than mere statistics—they are a reality. She argued that her traumatic experience could have been altogether avoided had Match.com warned her of the complaints it had received from other women about being violently attacked by the perpetrator.[8]

Given the association between social media threats and injury, the law should be equipped to hold social media companies accountable for their role in certain harms.[9] However, there are significant roadblocks that make it difficult for plaintiffs to get redress against online providers—namely, § 230 of the Communications Decency Act of 1996[10] (CDA) and the lack of precedent on how preexisting law should apply to internet cases.[11] To survive § 230 preemption, plaintiffs have attempted to argue that social media companies owe an affirmative duty of care to their users,[12] arising under the common law tort special relationship doctrine.[13] If the social media company and the injured user shared such a relationship, it may be possible to hold the social media company liable for failing to warn or protect that

2. Julie L. Valentine, Leslie W. Miles, Kristen M. Hamblin & Audrey W. Gibbons, *Dating App Facilitated Sexual Assault: A Retrospective Review of Sexual Assault Medical Forensic Examination Charts*, 38 J. INTERPERSONAL VIOLENCE 6298, 6299 (2022).

3. *Id.*

4. *See* Anna E. Garcia Whitlock, Brendan P. Gill, Joseph B. Richardson, Desmond U. Patton, Bethany Strong, Chidinma C. Nwakanma & Elinore J. Kaufman, *Analysis of Social Media Involvement in Violent Injury*, 158 JAMA SURGERY 1347 (2023).

5. *Id.* at 1348.

6. *Id.*

7. Beckman v. Match.com, LLC, No. 13-CV-97, 2017 WL 1304288, at *1 (D. Nev. Mar. 10, 2017), *aff'd*, 743 F. App'x 142 (9th Cir. 2018).

8. *See id.* at *1–2.

9. *See* Whitlock et al., *supra* note 4, at 1348.

10. Pub. L. No. 104-104, 110 Stat. 133 (codified in scattered sections of the U.S. Code); 47 U.S.C. § 230.

11. NetChoice, LLC v. Paxton, 142 S. Ct. 1715, 1716 (2022) (Alito, J., dissenting) (expressing concern about how preinternet precedents should apply to large social media companies).

12. *See* VALERIE C. BRANNON & ERIC N. HOLMES, CONG. RSCH. SERV., R46751, SECTION 230: AN OVERVIEW 13 (2024).

13. *See* Graham Smith, *Take Care with That Social Media Duty of Care*, INFORRM'S BLOG (Oct. 23, 2018), https://inforrm.org/2018/10/23/take-care-with-that-social-media-duty-of-care-graham-smith/ [https://perma.cc/RA7J-FGSE] (comparing social media to physical spaces where occupiers' liability may arise).

user.[14] Although courts have been reluctant to expand the duty to warn to encompass social media sites,[15] this Note argues that courts should reform how they evaluate duty and recognize that social media companies have "superior knowledge" about their customers that requires them to warn their users of known dangers. Such a decision would be grounded in doctrine and advisable from a policy standpoint as it would be consistent with tort law's aim to provide injured victims a means of recovery against their wrongdoer.[16]

Due to the variations in how courts determine the existence of a special relationship, this Note consolidates the discussion around the special relationship doctrine and advocates for a framework that enables victims to hold social media companies liable for certain harms incurred on or facilitated by social media platforms. This Note will review the various factors that are relevant to the special relationship analysis and urge more courts to consider the expansive knowledge possessed by social media companies when performing this analysis. Part I discusses social media and data mining practices, the history and scope of § 230, the policies underlying tort law duty of care and the special relationship doctrine, and recent cases involving assertions of a special relationship between a social media company and a user. Part II examines the various factors, in both internet and noninternet cases, that courts look at when deciding whether a special relationship exists between two parties. Finally, Part III argues that courts should be more willing to recognize the existence of special relationships between social media companies and their users, and advocates for more courts to incorporate a superior knowledge factor into their analyses.

I. THE BACKGROUND OF INTERNET LAWSUITS AND TORT LAW SPECIAL RELATIONSHIPS

Recognizing the difficulty that courts face when attempting to regulate online platforms requires an understanding of modern social media and the mandates of § 230 of the CDA. Part I.A describes the ubiquity of social media today, as well as information-gathering practices that are often employed by social media companies. Part I.B presents an overview of § 230 that covers its history, scope, and the current debate over its application. To understand the role of tort law in internet lawsuits, Part I.C provides background on the general philosophies underlying tort law, the duty to warn or protect, and the special relationship doctrine. Finally, Part I.D introduces a case concerning the intersection of the duty to warn, the internet, and § 230.

14. *See* Doe v. Internet Brands, Inc., 824 F.3d 846, 852 (9th Cir. 2016) (holding that § 230 would not bar the plaintiff's claim if she could successfully prove that the defendant company shared a special relationship with her).

15. *See* discussion *infra* Part II.A.

16. *See* Julia Brodsky, *The Big Idea: Torts Are Wrongs*, FORDHAM L. NEWS (July 7, 2020), https://news.law.fordham.edu/blog/2020/07/07/the-big-idea-torts-are-wrongs/ [https://perma.cc/E7JR-6R3D].

A. Social Media and Data Mining Practices

Internet users can generally recognize a social media platform when they see it, but the actual parameters of what social media is can be nebulous.[17] Social media is defined as "a form of mass media communications on the Internet . . . through which users share information, ideas, personal messages, and other content (such as videos)."[18] A social media platform typically falls within one of four categories: social networks, media-sharing networks, discussion forums, and consumer reviews.[19] Social networks, like Facebook and Twitter, enable users to foster relationships with friends, family, and total strangers.[20] Media-sharing networks, like Instagram and TikTok, are primarily used to share various types of media, such as photographs and videos.[21] Discussion forums, such as Reddit, permit users to ask questions, give advice, and generally communicate with other users.[22] Finally, consumer reviews, like Yelp or Tripadvisor, provide a space for users to share their experiences with a specific product, brand, or service.[23] Together, these forms of social media have revolutionized the public's ability to interact with one another and with businesses.[24] A recent survey revealed that approximately 68 percent of Americans actively use social media, and the typical social media user interacts with approximately 6.8 different platforms.[25] This usage has resulted in billions of dollars of revenue for popular social media companies.[26] In 2023, Facebook generated 134.9 billion dollars,[27] Instagram generated 49.8 billion dollars,[28] TikTok

17. *What Is Social Media?*, MCKINSEY & CO. (June 8, 2023), https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-social-media [https://perma.cc/4DCQ-X9QD].

18. *Social Media*, ENCYC. BRITANNICA, https://www.britannica.com/topic/social-media [https://perma.cc/E9KT-VXMK] (last visited Mar. 7, 2025). Social networking is usually understood as users building communities among themselves, whereas social media primarily involves using platforms to build an audience; however, this Note will use the term "social media" to encompass both concepts.

19. *See What Is Social Media?*, *supra* note 17.

20. *Id.*

21. *Id.*

22. *Id.*

23. *Id.*

24. *See id.*

25. Shubham Singh, *How Many People Use Social Media (2025 Statistics)*, DEMANDSAGE (Dec. 26, 2024), https://www.demandsage.com/social-media-users/ [https://perma.cc/W84D-R7GU].

26. *See infra* text accompanying notes 27–30.

27. Press Release, Meta, Meta Reports Fourth Quarter and Full Year 2023 Results; Initiates Quarterly Dividend (Feb. 1, 2024), https://s21.q4cdn.com/399680738/files/doc_news/Meta-Reports-Fourth-Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend-2024.pdf [https://perma.cc/JKZ8-M9PY].

28. Mansoor Iqbal, *Instagram Revenue and Usage Statistics (2025)*, BUSINESS OF APPS (Jan. 22, 2025), https://www.businessofapps.com/data/instagram-statistics/ [https://perma.cc/Z9P5-TF52].

generated 16.1 billion dollars,[29] and Match Group generated 3.3 billion dollars.[30]

The nature of social media blurs the line between the real and the online world.[31] Thus, social media data has uniquely enabled data scientists to integrate behavioral theories with computational methods to study how individuals interact and communities form.[32] This has led to the development of social media mining, the process of using data generated from social interactions online to analyze and represent meaningful patterns.[33] Through the use of various calculations and methodologies,[34] data scientists attempt to answer questions such as: "Who are the most important people in a social network?" "How can we recommend content or friends to individuals online?" "How can we analyze the behavior of individuals online?"[35] Utilizing a wide array of tools, social media companies are able to access a substantial amount of information about their users and apply that information to refine their business models. For instance, social media companies can track user data beyond direct interactions with their sites[36] by using third-party tracking to analyze a user's online activity long after the user leaves the website.[37] Some social media companies can also capture a user's appearance by using image and voice recognition.[38] For example, despite receiving backlash in 2021 for using a facial recognition system, Meta is planning to bring the feature back to fight scams and aid in account recovery.[39] Additionally, social media companies can associate user data with the particular geolocation it originated from, which enables analysts to create powerful models that can track the flu,

29. Mansoor Iqbal, *TikTok Revenue and Usage Statistics (2025)*, BUSINESS OF APPS (Jan. 22, 2025), https://www.businessofapps.com/data/tik-tok-statistics/ [https://perma.cc/N2NP-74G8].

30. Stacy J. Dixon, *Annual Revenue of the Match Group from 2012 to 2023*, STATISTA (Feb. 26, 2024), https://www.statista.com/statistics/449432/annual-dating-revenue-match-group/ [https://perma.cc/KGH2-ZCRH].

31. *See* Sherry Thomas, *A Virtual Life: How Social Media Changes Our Perceptions*, INSIGHT MAG. (Oct. 7, 2016), https://www.thechicagoschool.edu/insight/from-the-magazine/a-virtual-life/ [https://perma.cc/HZ94-FFN3].

32. HUAN LIU, MOHAMMAD A. ABBASI & REZA ZAFARANI, SOCIAL MEDIA MINING: AN INTRODUCTION 16 (2014).

33. *Id.* at 21.

34. *See generally id.*

35. *Id.* at 18–19.

36. *See infra* notes 37–40.

37. *How Websites and Apps Collect and Use Your Information*, FED. TRADE COMM'N CONSUMER ADVICE (Sept. 2023), https://consumer.ftc.gov/articles/how-websites-and-apps-collect-and-use-your-information [https://perma.cc/L5TB-APQ9].

38. Andriy Slynchuk, *Big Brother Brands Report: Which Companies Access Our Personal Data the Most?*, CLARIO (Nov. 29, 2022), https://clario.co/blog/which-company-uses-most-data/ [https://perma.cc/CC4D-H6K4].

39. *See id.*; *see also* Karissa Bell, *Meta Is Bringing Back Facial Recognition with New Safety Features for Facebook and Instagram*, ENGADGET (Oct. 21, 2024), https://www.engadget.com/social-media/meta-is-bringing-back-facial-recognition-with-new-safety-features-for-facebook-and-instagram-222523426.html [https://perma.cc/S3KA-WCQT].

predict elections, or observe linguistic differences between groups.[40] Although social media companies perform extensive research on their users, they do attempt to use data mining to provide some regulation and transparency on their platforms.[41] For example, Instagram has begun identifying and labeling certain content as generated by artificial intelligence, which displays a message on or above the image to warn users.[42]

The recency and complexity of social media data mining has created differing opinions on how certain tools, like algorithms, should be viewed under the law. The Supreme Court in *Gonzalez v. Google*[43] considered the question of whether YouTube was liable for aiding and abetting a terrorist attack when its algorithm recommended Islamic State of Iraq and Syria (ISIS) videos to interested users.[44] During oral arguments, Justice Thomas suggested that algorithms are merely content-neutral functions that treat pro-ISIS propaganda the same way as rice pilaf recipes.[45] However, in an amicus brief supporting neither party, the Lawyers' Committee for Civil Rights Under Law asserted that "there is nothing neutral about a recommendation algorithm that takes different data about different people in different contexts and provides those people with different outcomes—as its human designers instructed it to do."[46]

B. Overview and Scope of § 230

Much of the ambiguity surrounding social media and internet cases stems from a small section from the CDA[47] that has been referred to as "the 26 words that created the internet."[48] Section 230, specifically subsection (c), contains two provisions that together grant broad immunity to internet providers from suits related to content posted by their users.[49] Section 230(c)(1) states that: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by

40. DAVID JURGENS, TYLER FINETHY, JAMES MCCORRISTON, YI TIAN XU & DEREK RUTHS, GEOLOCATION PREDICTION IN TWITTER USING SOCIAL NETWORKS: A CRITICAL ANALYSIS AND REVIEW OF CURRENT PRACTICE 188 (2021), https://ojs.aaai.org/index.php/ICWSM/article/view/14627/14476 [https://perma.cc/TV75-J7BP].

41. *See* Jonathan Freger, *Lessons in Content Moderation from Popular Social Media Platforms*, FORBES (May 23, 2024, 7:30 AM), https://www.forbes.com/councils/forbestechcouncil/2024/05/23/lessons-in-content-moderation-from-popular-social-media-platforms/ [https://perma.cc/K3AM-LXWU].

42. *Label AI Content on Instagram*, INSTAGRAM HELP CTR., https://help.instagram.com/761121959519495 [https://perma.cc/355G-8JU8] (last visited Mar. 7, 2025).

43. 143 S. Ct. 1191 (2023).

44. *Id.* at 1191–99; *see* Gonzalez v. Google LLC, 2 F.4th 871, 881 (9th Cir. 2021).

45. *See* Transcript of Oral Argument at 6–7, *Gonzalez*, 143 S. Ct. 1191 (No. 21-1333).

46. Brief of The Lawyers' Committee for Civil Rights Under Law and Five Civil Rights Organizations as Amici Curiae in Support of Neither Party at 18, *Gonzalez*, 143 S. Ct. 1191 (No. 21-1333).

47. Communications Decency Act, Pub. L. No. 104-104, 110 Stat. 133 (1996).

48. *See* Brian Fung, *These 26 Words 'Created the Internet.' The U.S. Government Is Coming for Them*, CNN (Feb. 25, 2020, 12:10 PM), https://www.cnn.com/2020/02/25/tech/section-230-doj/index.html [https://perma.cc/QH2Z-7D3F].

49. BRANNON & HOLMES, *supra* note 12, at 8.

another information content provider."[50] Section 230(c)(2) ensures that internet providers will not be held liable for good faith efforts to moderate content.[51] The statute defines an "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server."[52] Today, most interactive computer services are websites.[53] Part I.B.1 will briefly introduce § 230 by explaining its history and how courts have interpreted it. Part I.B.2 will then discuss the current debates regarding its scope.

1. The History of § 230

According to the Senate conference report, the CDA was enacted to "modernize the existing protections against obscene, lewd, indecent or harassing uses of a telephone."[54] Following concerns about free speech and the rising prevalence of internet platforms, Congress amended the CDA to include § 230.[55] Section 230's language expresses its goals to "promote the continued development of the internet, . . . remove disincentives for the development . . . of blocking and filtering technologies, . . . [and] ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer."[56]

The origins of § 230 can be traced back to two New York court decisions[57] in the early 1990s that lawmakers were concerned would disincentivize online content moderation.[58] Together, those cases suggested that an internet provider that attempted to regulate third-party content on its website could be more vulnerable to lawsuits than an internet provider that did not monitor its content at all.[59] To address this, § 230 was added as an amendment to the CDA to shield online platforms from liability for third-party content in order to encourage websites to continue and develop moderation practices.[60]

---

50. 47 U.S.C. § 230(c)(1).

51. *Id.* § 230(c)(2); *see infra* text accompanying notes 57–58.

52. *Id.* § 230(f)(2).

53. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1162 (9th Cir. 2008).

54. S. REP. NO. 104-23, at 59 (1995).

55. *Section 230: Legislative History*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/cda230/legislative-history#main-content [https://perma.cc/22P6-L25K] (last visited Mar. 7, 2025).

56. 47 U.S.C. § 230(b).

57. *See* Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991); *see also* Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). In *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991), the operator of an online forum was not liable for libel by a third-party user because it neither knew, nor had reason to know, of the defamatory statements because it did not review any of the content posted on its forums. *Cubby*, 776 F. Supp. at 141. In *Stratton Oakmont, Inc. v. Prodigy Services Co.*, No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), the operator of online bulletin boards was found liable for third-party messages because the operator claimed to exercise editorial control over the content on its site. *Prodigy*, 1995 WL 323710, at *3.

58. *See* BRANNON & HOLMES, *supra* note 12, at 7–8.

59. *Id.*

60. *Id.* at 2; *see* S. REP. NO. 104-23, at 9 (1995).

2. The Scope of § 230 Immunity

Since its enactment, courts have interpreted § 230 broadly to shield internet providers from liability.[61] The first major judicial interpretation of § 230 was in *Zeran v. America Online, Inc.*[62] This case involved an unidentified user on AOL who posted advertisements for shirts celebrating the Oklahoma City bombing and invited interested buyers to call the plaintiff, Zeran, at his home phone.[63] Concerned with the chilling effects that could result from holding internet providers liable for each of their users' many postings, the U.S. Court of Appeals for the Fourth Circuit held that websites are generally immune from liability for unlawful or harmful third-party content.[64] This holding presented a broad view of § 230 that other courts of appeals have largely adopted.[65] However, the broad immunity set forth in *Zeran* is not absolute—there are carve outs for federal crimes, intellectual property laws, and certain state, privacy, and sex-trafficking laws.[66]

But because the internet has evolved far beyond what it was in 1996, commenters have raised concerns that § 230 has not grown to reflect the modern reality of the digital age.[67] Critics argue that § 230's protections are overbroad or unwarranted and allow online service providers to facilitate criminal behavior without fear of liability.[68] Additionally, two federal appellate judges have questioned, in separate § 230 cases, whether *Zeran*'s definition of a publisher extended § 230(c)(1) beyond its intended scope.[69]

Meanwhile, defenders of the law argue that a broad application of § 230 is necessary to protect free expression on the internet because it allows online service providers to freely host content without having to review each post for potential legal issues.[70] They contend that this is important because the internet enables large-scale communication and was recognized by the Supreme Court as one of "the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and

61. BRANNON & HOLMES, *supra* note 12 at 8.
62. 129 F.3d 327 (4th Cir. 1997).
63. *Id.* at 329.
64. *Id.* at 333.
65. BRANNON & HOLMES, *supra* note 12, at 10.
66. Randi Singer & Liz McLean, *Section 230's Original Intent Offers Touchstone for Online Safety*, BLOOMBERG L. (July 29, 2024, 4:30 AM), https://news.bloomberglaw.com/us-law-week/section-230s-original-intent-offers-touchstone-for-online-safety [https://perma.cc/V5CN-6S6W].
67. *See* KATHLEEN A. RUANE, CONG. RSCH. SERV., LSB10082, HOW BROAD A SHIELD?: A BRIEF OVERVIEW OF SECTION 230 OF THE COMMUNICATIONS DECENCY ACT 1 (2018), https://crsreports.congress.gov/product/pdf/LSB/LSB10082 [https://perma.cc/93G5-GJT7].
68. *Id.*
69. *See, e.g.*, Force v. Facebook, Inc., 934 F.3d 53, 84 (2d Cir. 2019) (Katzmann, J., concurring in part) (opining that the current application of § 230 extends immunity for activities that were unimaginable in 1996); *see also* Gonzalez v. Google LLC, 2 F.4th 871, 915 (9th Cir. 2021) (Berzon, J., concurring) (finding that the legislative history of § 230 does not support a broad reading of publisher functions).
70. RUANE, *supra* note 67, at 1.

knowledge."[71] Thus, according to § 230 advocates, without the protections of § 230, important topics of speech—especially concerning inflammatory subjects such as race and racism, sexuality, politics, and gender justice—may become overly censored if internet platforms are primarily concerned with guarding against possible defamation suits.[72]

Even the Supreme Court has struggled to define the scope of § 230 and apply prior case law to novel internet issues.[73] As Justice Kagan observed, "[The justices] really don't know about these things . . . these are not like the nine greatest experts on the internet."[74] However, some recent Supreme Court decisions suggest there may be some movement in favor of limiting § 230's protections. For instance, in *Malwarebytes, Inc. v. Enigma Software Group U.S.A., LLC*,[75] the Court, in denying a petition for a writ of certiorari, held that paring back the broad application of § 230 would not necessarily render the defendants liable, but would simply give the plaintiffs an opportunity to raise their claims.[76] Another example is *Twitter v. Taamneh*,[77] where the Supreme Court considered whether Twitter could be liable for aiding and abetting a terrorist attack by providing ISIS a platform on its website and connecting users to ISIS through its algorithm system.[78] Though the Court ultimately decided that the plaintiffs failed to demonstrate that the defendants intentionally aided or participated in the attack,[79] Justice Jackson's concurrence emphasized that the *Taamneh* holding was narrow,[80] and the majority opinion expressed that the plaintiffs' claims might have had greater purchase if they were able to identify an independent duty in tort law that would require Twitter (now X) to remove ISIS content.[81] The Court noted that there may be situations where such a duty exists, though they declined to resolve that issue in *Taamneh*.[82]

71. Packingham v. North Carolina, 137 S. Ct. 1730, 1732 (2017).

72. Jennifer S. Granick, *Is This the End of the Internet As We Know It?*, ACLU (Feb. 22, 2023), https://www.aclu.org/news/free-speech/section-230-is-this-the-end-of-the-internet-as-we-know-it [https://perma.cc/T8QA-MLA5].

73. *See* Netchoice, LLC v. Paxton, 142 S. Ct. 1715, 1717 (2022) (Alito, J., dissenting) (noting that "[i]t is not at all obvious how our existing precedents, which predate the age of the internet, should apply to large social companies").

74. *See* Transcript of Oral Argument, *supra* note 45 at 45–46.

75. 141 S. Ct. 13 (2020).

76. *Id.* at 18.

77. 143 S. Ct. 1206 (2023).

78. *Id.* at 1214.

79. *Id.* at 1231.

80. *Id.* at 1231 (Jackson, J., concurring).

81. *Id.* at 1227 (majority opinion).

82. *Id.* at 1227–28.

C. Tort Law and the Special Relationship Doctrine

Tort law, such as defamation[83] or products liability claims,[84] has been applied to internet cases with varying success as the existing common law may be ill-equipped to address internet-based activities.[85] This section will (1) discuss the underlying principles of tort law, (2) elaborate on the duty of care, and (3) explain the special relationship doctrine and its emergence within internet law.

1. Basic Tort Principles

One of the fundamental principles of tort law is that for every legal wrong, victims should be entitled to seek recourse against their wrongdoer.[86] Tort law also places liability on the party that is best able to determine the cost-justified level of injury prevention.[87] It serves at least three functions: compensating plaintiffs for injuries resulting from wrongful conduct, deterring society at large from acting in a harmful manner, and serving as a method for punishing those who wrongfully injure others.[88] With a few exceptions, tort law is primarily a matter of state law rather than federal law and is derived from common law rather than statutory law.[89] As a result, different jurisdictions may vary in their analyses of what constitutes tortious conduct, but the broad doctrinal aims of tort law remain fairly uniform.[90] They lay out the minimal standards of conduct that people are allowed to legally demand of each other and enable those who have been harmed to seek remedies from those who have harmed them.[91]

These aims may have roots in morality and fairness. In his 1881 book, *The Common Law*, Oliver Wendell Holmes Jr., noted that tort law is abundant with moral phraseology, but it only imposes external standards that take moral considerations into account to determine what kinds of actions or

83. *See* Leslie Y. Garfield Tenzer, *Social Media Harms and the Common Law*, 88 BROOK. L. REV. 227, 245–48 (2022).

84. Danny Barefoot, William Oxley & Meghan Rohling Kelly, *Social Media Firms Navigate Product Liability Claims*, BLOOMBERG L. (Sept. 28, 2022, 4:00 AM), https://news.bloomberglaw.com/us-law-week/social-media-firms-navigate-product-liability-claims [https://perma.cc/76B8-DCGQ].

85. MARY MULLEN, HOUSE RSCH. DEP'T, THE INTERNET AND PUBLIC POLICY: CYBERTORTS AND ONLINE PROPERTY RIGHTS (May 2018), https://www.house.mn.gov/hrd/pubs/int_cybertort.pdf [https://perma.cc/2GMN-N3NP].

86. *See* Brodsky, *supra* note 16.

87. Banks v. Hyatt Corp., 722 F.2d 214, 226 (5th Cir. 1984).

88. *See* ANDREAS KUERSTEN, CONG. RSCH. SERV., IF1191, INTRODUCTION TO TORT LAW (2023), https://crsreports.congress.gov/product/pdf/IF/IF11291 [https://perma.cc/7JY5-AY6A].

89. *Id.*

90. *See* Arthur Ripstein, *Theories of the Common Law of Torts*, STAN. ENCYCLOPEDIA PHIL. (June 2, 2022), https://plato.stanford.edu/entries/tort-theories/ [https://perma.cc/R2WZ-EXM9].

91. *Id.*

omissions are permissible.[92] For instance, tort law often applies a "reasonable person" standard to determine whether unlawful behavior has occurred in a particular instance.[93] Although subject to criticism,[94] the objective of the reasonable person standard is to establish a link between the law and what is considered ordinary or normal behavior, for that particular person or entity, within society.[95]

2. The Duty of Care

The reasonable person standard typically arises when discussing a person's duty of care toward others in the context of a negligence claim.[96] There is no set definition of duty, as it is a judgment of law.[97] As stated in *Dillon v. Legg*,[98] the essential question of duty is whether the plaintiff's interests are entitled to legal protection against the defendant's conduct—duty is simply an expression of the policy considerations allowing a plaintiff to receive legal protection.[99]

In most cases, the duty of care for anyone who undertakes an affirmative act is that of a reasonable person to protect others from an unreasonable risk of harm arising out of the act.[100] In deciding whether the defendant owed a duty of care to the plaintiff, case law distinguishes "misfeasance," a wrongful affirmative act, from "nonfeasance," a failure to act in the face of a duty to do so.[101] Generally, the mere realization that some action is necessary to aid or protect another does not itself impose a duty upon an individual to take such action[102] because tort law typically does not impose an affirmative duty to warn, protect, or rescue others.[103] The traditional duty of care also does not include a duty to protect third parties.[104] However, certain dynamics may exist between the actor and another that imposes on the actor a duty to act affirmatively to aid or protect the other.[105] This duty to aid or protect may

92. *See generally* OLIVER WENDELL HOLMES, JR., THE COMMON LAW 79–110 (Little, Brown & Co. ed., 1881).

93. *See, e.g.*, Universal Health Servs., Inc. v. United States, 136 S. Ct. 1989, 2003 (2016) (explaining that, for fraudulent misrepresentation, a matter is material if a reasonable person would attach importance to it).

94. For further discussion, see Alan D. Miller & Ronen Perry, *The Reasonable Person*, 87 N.Y.U. L. REV. 323 (2012).

95. Mayo Moran, The Reasonable Person: A Conceptual Biography in Comparative Perspective, 14 LEWIS & CLARK L. REV. 1233, 1236 (2010).

96. *Negligence*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/negligence [https://perma.cc/KX2F-SA4W] (last visited Mar. 7, 2025).

97. See Theodore R. Boehm, *A Tangled* Webb*—Reexamining the Role of Duty in Indiana Negligence Actions*, 37 IND. L. REV. 1, 6 (2003).

98. 441 P.2d 912 (Cal. 1968).

99. *See id.* at 916.

100. RESTATEMENT (SECOND) OF TORTS § 302, cmt. a (AM. L. INST. 1965).

101. *Id.*

102. *See* RESTATEMENT (SECOND) OF TORTS § 314.

103. Kenneth S. Abraham & Leslie Kendrick, *There's No Such Thing As Affirmative Duty*, 104 IOWA L. REV. 1649, 1656–57 (2019).

104. *See* RESTATEMENT (SECOND) OF TORTS § 315.

105. *See id.* § 314A.

also extend to third parties if the actor had a special relationship with either the bad actor or the third-party victim.[106]

3. The Special Relationship Exception

Where an individual is deemed to have a legal "special relationship" with another, the law creates an exception to the general rule that there is no affirmative duty to warn and requires the individual to take reasonable steps to protect the other person.[107] There are four explicit types of special relationships: (1) common carriers to their passengers, (2) innkeepers to their guests, (3) landowners who hold their land open to members of the public who enter in response to an invitation, and (4) custodians to their ward.[108] These special relationships typically involve a vulnerable individual subject to the actions or oversight of another. For example, the innkeeper-guest relationship stemmed from courts analogizing it to the common carrier–passenger relationship because innkeepers' contracts impose a similar duty to protect guests.[109] This is because guests are peculiarly at the mercy of innkeepers and their employees.[110] But where guests are injured by other guests, innkeepers are absolved of liability unless they knew or should have known that offending guests were likely to injure other guests, in which case innkeepers must take reasonable steps to prevent the harm.[111] This is because innkeepers are in the best position to take preventative action to guard against the predictable risk of assaults.[112] In addition to these enumerated categories, courts will sometimes find that the facts of a case give rise to a special relationship between two parties.[113] This usually requires the court to determine whether the relationship between the defendant and the victim gives the victim a right to expect protection from the defendant or whether the relationship between the defendant and the dangerous individual is one that involves an ability to control the dangerous individual.[114]

The Supreme Court of California expanded the special relationship duty to third-party victims by requiring doctors and therapists to warn a potential victim if a patient threatens harm to them. In *Tarasoff v. Regents of the University of California*,[115] Prosenjit Poddar killed Tatiana Tarasoff two months after confiding his intention to kill Tarasoff to his psychologist, who was employed by the University of California, Berkeley.[116] The plaintiffs,

106. *See id.*
107. *Id.*
108. RESTATEMENT (SECOND) OF TORTS § 314A.
109. See Edward Louis Eyerman, *The Modern Innkeeper's Liability for Injuries to the Person of His Guest*, 19 ST. LOUIS L. REV. 232, 234–35 (1934).
110. *See id.* at 235.
111. *See id.*
112. Banks v. Hyatt Corp., 722 F.2d 214, 225–26 (5th Cir. 1984).
113. *See* Thompson *ex rel*. Thompson v. Skate America, Inc., 540 S.E.2d 123, 127 (Va. 2001) (listing cases where special relationships were found de jure or de facto).
114. *See* Brown v. USA Taekwondo, 483 P.3d 159, 166 (Cal. 2021).
115. 551 P.2d 334 (Cal. 1976).
116. *Id.* at 339.

Tarasoff's parents, claimed that the defendants were negligent in failing to warn them of the impending danger posed by Poddar.[117] The defendants contended that imposing a duty to exercise reasonable care to protect a third person is unworkable. The court rejected the defendants' reasoning and found that the role of a psychologist is to make diagnoses and predictions based on evaluating a patient, so the defendants were reasonably able to identify and warn Tarasoff of a danger arising from those predictions.[118] In comparing the burden on the defendant to the potential benefits of imposing such a duty, the court decided that the lives of potential victims outweighed the risk of issuing unnecessary warnings.[119] The court further concluded that doctor-patient confidentiality protections must yield to the extent that disclosure is essential to preventing danger to the public.[120] Therefore, the court established a special relationship that requires doctors to act for the benefit of reasonably identifiable third parties.[121] Many states have established a *Tarasoff* duty to warn, but the guidelines for reporting vary widely between and within states.[122]

D. The Duty to Warn for Social Media Companies

The special relationship exception has been raised in a few internet cases where the social media company knew that a dangerous user was likely to harm another user.[123] In 2016, the U.S. Court of Appeals for the Ninth Circuit decided a case in which an injured plaintiff alleged that a social networking website had a special relationship with her. *Doe v. Internet Brands, Inc.*[124] involved an aspiring model who marketed herself on a networking site for the modeling industry, through which she was contacted by two users who ultimately drugged and raped her.[125] The website, "Model Mayhem," was owned by Internet Brands and had over 600,000 users, including Lavont Flanders and Emerson Callum, who did not post their own profiles on the website but used it to identify targets for their rape scheme, allegedly beginning as early as 2006.[126] The two contacted potential victims while posing as talent scouts, lured them to Florida for so-called modeling auditions, then drugged their victims before raping them and recording the

117. *Id.* at 340.
118. *Id.* at 345.
119. *Id.* at 346.
120. *Id.* at 347.
121. *Id.*
122. Twenty-three states have statutorily mandated reporting laws, eleven states have the duty to warn as common law, eleven states are permissive toward the duty to warn, and six states have no guidance on the *Tarasoff* warning. Olga Gorshkalova & Sunil Munakomi, *Duty to Warn*, NAT'L LIBR. OF MED. (Aug. 28, 2023), https://www.ncbi.nlm.nih.gov/books/NBK542236/ [https://perma.cc/L7YT-YYXF].
123. *See infra* Part II.A.
124. 824 F.3d 846 (9th Cir. 2016).
125. *Id.* at 848.
126. *Id.*

activity to sell as pornography.[127] The website allegedly learned of this criminal activity in 2010 through an outside source, not from monitoring postings on the website.[128] Doe sued Internet Brands, claiming that it had a special relationship with her and that its failure to warn her about the rape scheme caused her to fall victim to it.[129]

The Ninth Circuit reversed the district court's dismissal of the case, holding that the CDA did not bar the claim because the plaintiff did not seek to hold the website liable as a "publisher or speaker" of content or for failure to remove content, and because the predatory activity was discovered through a third party rather than by the platform monitoring postings.[130] However, the court expressed no opinion on the merits of her failure-to-warn claim nor on the existence of the requisite special relationship.[131] On remand,[132] the U.S. District Court for the Central District of California found that Internet Brands did not have a special relationship with Doe.[133]

Though there are concerns about the consequences of imposing a duty of care on social media companies, there is also support for holding the social media industry to a higher degree of accountability. For instance, in *Godwin v. Facebook, Inc.*,[134] Judge Patricia Ann Blackmon expressed worry in her concurrence over the lack of law governing the relationship between social media companies and their users.[135] She expressed that there is a duty owed by social media companies to their users and that the law of torts is elastic so that the concept of "duty" adapts to advancements in society.[136] Therefore, public policy and public opinion should determine what constitutes a special relationship.[137] She noted that the extent to which social media companies "take[] charge" of their users remains unknown (at the time of the case), but their influence on modern day society is indisputable.[138] Judge Blackmon concluded by writing that "only when legal and moral duty diverge can courts hear a call for movement and reform."[139]

127. *Id.*
128. *Id.* at 849.
129. *Id.*
130. *Id.* at 851.
131. *Id.* at 854.
132. Doe No. 14 v. Internet Brands, Inc., No. CV 12-3626, 2016 WL 11824793 (C.D. Cal. Nov. 14, 2016).
133. *Id.* at *5.
134. 160 N.E.3d 372 (Ohio Ct. App. 2020).
135. *Id.* at 386.
136. *Id.* For example, in 1983, the Supreme Court of Ohio recognized negligent infliction of serious emotional distress as a valid cause of action for the first time. *See* Paugh v. Hanks, 451 N.E.2d 759, 762 (Ohio 1983).
137. *Godwin*, 160 N.E.3d at 387.
138. *Id.*
139. *Id.* at 388.

II. FACTORS COURTS CONSIDER IN A SPECIAL RELATIONSHIP ANALYSIS

Social media cases have been particularly difficult for courts to decide due to the novelty of the issues presented and, therefore, the lack of precedent.[140] This is especially true in the context of special relationship arguments; only a few cases have dealt with this question and, thus far, no court has affirmatively ruled that a social media company has a special relationship to an injured user.[141] However, such a finding is not foreclosed.[142] Part II will discuss the relevant factors that courts have considered when deciding whether a special relationship exists. Part II.A will describe social media cases where the court has analyzed the special relationship question. Part II.B will then turn to potentially analogous noninternet cases where a special relationship was recognized and assess what factors courts considered to arrive at such a conclusion.

A. Internet Special Relationship Cases

Courts have traditionally hesitated to extend the special relationship doctrine beyond its established categories, especially in internet cases involving a failure to act.[143] This section will examine cases where plaintiffs argued that a social media company had a special relationship with them and note which factors the courts found relevant when declining to recognize a special relationship. The focus of this discussion will center primarily around three cases from the Ninth Circuit and will also assess another notable case pending in Florida.

1. Analyses of Courts Within the Ninth Circuit

As mentioned in Part I.D, the Ninth Circuit remanded *Internet Brands* to assess the viability of the plaintiff's duty to warn claim.[144] There, the Central District of California dismissed the action by ruling that Internet Brands did not have a special relationship with Doe, finding no affirmative duty of care that required it to warn her about the rape scheme.[145] The court first rejected the notion that Internet Brands "created" the peril or risk by failing to warn Doe, stating that merely allowing members to use the site without warning

140. *See* NetChoice, LLC v. Paxton, 142 S. Ct. 1715, 1717 (2022) (Alito, J., dissenting) (expressing concerns over the novelty of internet cases and the difficulty applying preinternet precedent to them).

141. *See, e.g.*, Doe No. 14 v. Internet Brands, Inc., No. CV 12-3626, 2016 WL 11824793 (C.D. Cal. Nov. 14, 2016) (declining to create a special relationship); Dyroff v. Ultimate Software Grp., Inc., 934 F.3d 1093 (9th Cir. 2019) (declining to create a special relationship); *Godwin*, 160 N.E.3d 372 (rejecting plaintiff's special relationship argument).

142. *See* Twitter, Inc. v. Taamneh, 143 S. Ct. 1206, 1221 (2023) (holding that plaintiff failed to identify an independent duty to act, but that there may be situations where such a duty exists).

143. *See Doe No. 14*, 2016 WL 11824793, at *5.

144. Doe v. Internet Brands, Inc., 824 F.3d 846, 849–54 (9th Cir. 2016).

145. *Doe No. 14*, 2016 WL 11824793, at *5.

them of the rape scheme did not alone create risk or peril, thus eliminating the possibility of a duty of care arising out of any misfeasance by Internet Brands.[146] The court explained that a duty of care may arise from either "(a) a special relation between the actor and the third person which imposes a duty upon the actor to control the third person's conduct, or (b) a special relation between the actor and the other which gives to the other a right of protection."[147] Therefore, in order to establish liability for Internet Brands' nonfeasance, Doe had to prove that Internet Brands either had a special relationship with Flanders and Callum or with her.[148] The court quickly dismissed the issue of whether Internet Brands had a special relationship with the perpetrators, an allegation that Doe did not even make in her claim.[149] Then, focusing on the relationship between Internet Brands and Doe, the court first noted that the website operator–user relationship does not fall under any of the recognized special relationships under California law, and the court had not located, nor was Doe able to cite, any case where courts found the existence of a special relationship under analogous circumstances.[150] The court also looked at the factors set out in *Rowland v. Christian*,[151] the leading California case on special relationships, and concluded that existing case law and application of the *Rowland*[152] factors did not justify creating a special relationship in this instance.[153] The court analogized to *Conti v. Watchtower Bible & Tract Society of New York, Inc.*,[154] where the California Court of Appeals held that there was no "special relationship" duty that required a church to inform its congregation that a fellow member was a child molester.[155] The court in *Conti* admitted that harm to child members was foreseeable, but was outweighed by the impracticality of requiring a church to issue warnings to all of its members whenever it believed a member was capable of doing harm, especially because the scope of such a duty would be difficult to define.[156] Similarly,

146. *Id.* at *4.
147. *Id.*
148. *Id.* at *5.
149. *Id.*
150. *Id.*
151. 443 P.2d 561 (Cal. 1968).
152. The major factors are: (1) the foreseeability of harm to the plaintiff, (2) the degree of certainty that the plaintiff suffered injury, (3) the closeness of the connection between the defendant's conduct and the injury suffered, (4) the moral blame attached to the defendant's conduct, (5) the policy of preventing future harm, (6) the extent of the burden on the defendant and consequences to the community of imposing such a duty, and (7) the availability of insurance for the risk involved. *Rowland*, 443 P.2d at 564.
153. *Doe No. 14*, 2016 WL 11824793, at *5. In 2021, the Supreme Court of California clarified that the *Rowland* factors are to be considered *after* finding that a special relationship exists, in order to decide whether relevant policy considerations counsel limiting that duty. *See* Brown v. USA Taekwondo, 483 P.3d 159, 166–70 (9th Cir. 2021).
154. 186 Cal. Rptr. 3d 26 (Ct. App. 2015).
155. *Id.* at 38. Plaintiffs failed to assert that either: (1) members of a church have a special relationship with the church by virtue of their membership that requires the church to protect them from other members, or (2) a church has a special relationship with any member it believes may perpetrate harm. *Id.*
156. *Id.* at 39.

the *Internet Brands* court held that, although it may have been foreseeable that Flanders and Callum would harm another victim, Internet Brands only knew about the threat to its members at large, not to any specific member.[157] Thus, imposing a duty to warn here would not cause website users to adopt significantly greater precautions than they were already taking and would likely lead to the website overwhelming their users with warnings, which would dilute the warnings' effectiveness.[158] Finally, the court expressed concerns that imposing a duty to warn would open the floodgates of litigation and likely result in a "chilling" effect on the Internet.[159]

Around the time *Internet Brands* was decided, another social media case regarding special relationships was brought in the U.S District Court for the District of Nevada. In *Beckman v. Match.com, LLC*,[160] Mary Kay Beckman met Wade Ridley through Match's dating service.[161] When she ended their relationship less than ten days after their first date, Ridley sent her numerous threatening and harassing text messages.[162] Four months later, Ridley attacked her in her garage, stabbing her until his knife broke.[163] Beckman alleged that Match received complaints that Ridley had harassed, threatened, or violently attacked other women using Match's services and that, despite these complaints, Match allowed Ridley's profile to remain active.[164] Additionally, Beckman contended that Match had "unique access to information" and "utilized that data to create 'matches' among its users."[165]

In its analysis, the court noted that the existence of a special relationship is premised on "the ability of one of the parties to provide for his own protection" being "limited in some way by his submission to the control of another."[166] Furthermore, the court emphasized that this ability to protect must have been capable of meaningfully reducing the risk of harm at issue.[167] The court ruled that Beckman failed to plead facts giving rise to such a special relationship and that the complaint itself did not allege that a special relationship existed.[168] Any allegations that Match looked at, analyzed, judged, or paired Beckman and Ridley together were absent from the

157. *Doe No. 14*, 2016 WL 11824793, at *5.
158. *Id.*
159. *Id.*
160. No. 13-CV-97, 2017 WL 1304288 (D. Nev. Mar. 10, 2017), *aff'd*, 743 F. App'x 142 (9th Cir. 2018).
161. *Id.* at *1.
162. *Id.*
163. *Id.*; *see* Paul Rubin, *Wade Ridley, Match.com "Hunter" Who Killed Phoenix Woman, Apparently Commits Suicide in Nevada Joint*, PHX. NEW TIMES (May 17, 2012), https://www.phoenixnewtimes.com/news/wade-ridley-matchcom-hunter-who-killed-phoenix-woman-apparently-commits-suicide-in-nevada-joint-6644392 [https://perma.cc/HN3U-E54D].
164. *Beckman*, 2017 WL 1304288, at *1; *see also* Rubin, *supra* note 163 (noting that Ridley confessed to murdering another ex-girlfriend from Match, Anne Simenson, one month after Beckman's attack).
165. *Beckman*, 2017 WL 1304288, at *3.
166. *Id.* (quoting Sparks v. Alpha Tau Omega Fraternity, Inc., 255 P.3d 238, 245 (Nev. 2011)).
167. *Id.*
168. *Id.*

complaint.[169] Moreover, even if Beckman had been able to allege any of the above, the attack occurred months after Beckman and Ridley ended their relationship, and Beckman was allegedly aware of Ridley's dangerous nature prior to the attack, so Beckman's ability to protect herself was not limited in any way by her submission to Match's control.[170] For those reasons, the court held that there was no special relationship between Beckman and Match,[171] which was affirmed by the Ninth Circuit.[172]

The third case dealing with this issue is *Dyroff v. Ultimate Software Group, Inc.*,[173] where a (now dormant) social networking website called Experience Project, owned by Ultimate Software, allowed users to anonymously share their first-person experiences online and interact with other users about different topics.[174] Ultimate Software used advanced data mining algorithms to analyze posts and other user data to learn information (such as the underlying intent and emotional state of its users) for commercial purposes and to introduce users to new groups on the website through a recommendation function.[175] The plaintiff was the mother of Wesley Greer, who was addicted to opioids and posted a question on Experience Project inquiring about where he could find heroin nearby.[176] Shortly after posting, Experience Project notified Greer via email that Hugo Margenat-Castro, a drug dealer, had responded to his post.[177] Greer called Margenat-Castro and then met him to buy fentanyl-laced heroin.[178] Greer later died from fentanyl toxicity after using that heroin.[179] The investigation revealed that Margenat-Castro had regularly used Experience Project to sell heroin, posting numerous times in groups titled, "I love Heroin" and "heroin in Orlando."[180] Based on his activity on Experience Project, law enforcement arrested Margenat-Castro for possession with intent to sell fentanyl, stemming from his sale of drugs on the website.[181]

The plaintiff contended that, at the time her son bought the drugs, Ultimate Software had actual or constructive knowledge of the drug trafficking occurring on its site, but still permitted users to create groups dedicated to the sale and use of illegal narcotics.[182] Not only did it allow the drug-focused groups to exist, but it also used its algorithmic functions to steer vulnerable

169. *Id.*
170. *Id.*
171. *Id.* at *4.
172. *See* Beckman v. Match.com, LLC, 743 F. App'x 142, 143 (9th Cir. 2018).
173. No. 17-CV-05359, 2017 WL 5665670 (N.D. Cal. Nov. 26, 2017), *aff'd*, 934 F.3d 1093 (9th Cir. 2019).
174. *Id.* at *2.
175. *Id.*
176. *Id.*
177. *Id.* at *3.
178. *Id.*
179. *Id.*
180. *Id.*
181. *Id.* In his plea agreement, Margenat-Castro estimated that he sold ten bags of fentanyl-laced heroin every day (seven days a week) through Experience Project, resulting in approximately 1,400 total bags of fentanyl-laced heroin being sold. *Id.*
182. *Id.*

users to these harmful groups and allowed users to maintain active accounts on Experience Project, despite the platform's awareness of the drug trafficking and multiple law enforcement actions against users related to their activity on the website.[183] The court ruled that Ultimate Software did not have a special relationship with Greer that required it to warn him that Margenat-Castro was selling fentanyl-laced heroin and did not create the risk through its website's functionalities.[184] The court relied on the holdings in *Internet Brands* and *Beckman*, as well as the *Rowland* factors, to support its conclusion that websites do not have a "special relationship" with their users.[185] The court was unconvinced by the plaintiff's analogy that websites are like brick-and-mortar businesses open to the public that have a duty to take affirmative action to protect invitees when there's reasonable cause to anticipate an injury occurring.[186] The court was concerned, similarly to the court in *Internet Brands*, that following this approach would render all social media networks potentially liable whenever they connect their members through an algorithm, which would open the floodgates of litigation and likely result in a "chilling effect" on the internet.[187] Additionally, the court held that, even if Ultimate Software had superior knowledge about the fentanyl-laced heroin, knowledge does not create a special relationship absent dependency or detrimental reliance by its users, which was not alleged by the plaintiff.[188] On appeal, the Ninth Circuit affirmed the district court's holding, adding that no website could operate if a duty of care was created when it uses content-neutral functions to facilitate communication of its users' content.[189]

The above cases rejected the existence of a special relationship and pointed to the plaintiffs' inability to cite any relevant case law that expanded the special relationship under similar circumstances.[190] The Ninth Circuit focused largely on submission and reliance in their analyses, and voiced concerns about how such a requirement would operate practically.[191] They also emphasized slightly different aspects of the special relationship doctrine in their analyses. The District Court of Nevada in *Beckman* centered its discussion around the idea of "control and custody," finding that Match was too far removed from the attack for its relationship to Beckman or Ridley to

183. *Id.* at *3–4.
184. *Id.* at *1.
185. *Id.* at *13–14.
186. *Id.* at *14.
187. *Id.* (quoting Doe No. 14 v. Internet Brands, Inc., No. CV 12-3626, 2016 WL 11824793, at *5 (C.D. Cal. Nov. 14, 2016)).
188. *Id.* at *15.
189. Dyroff v. Ultimate Software Grp., Inc., 934 F.3d 1093, 1101 (9th Cir. 2019).
190. *Doe No. 14*, 2016 WL 11824793, at *5; *see also* Beckman v. Match.com, LLC, 743 F. App'x 142 (9th Cir. 2018) (stating that Nevada courts have never recognized a special relationship akin to that between Beckman and Match); Dyroff v. Ultimate Software Grp., Inc., No. 17-CV-05359, 2017 WL 5665670, at *13–14 (N.D. Cal. Nov. 26, 2017), *aff'd*, 934 F.3d 1093 (9th Cir. 2019) (relying on *Internet Brands* and *Beckman* to support a finding of no special relationship, while being unconvinced of plaintiff's analogy to brick-and-mortar businesses).
191. *See supra* Part II.A.1.

be characterized in such a way.[192] In *Internet Brands* and *Dyroff*, the U.S. District Courts for the Central and Northern Districts of California considered the *Rowland* factors and engaged in a slightly more policy-centered discussion, finding that because any warnings would likely only be minimally effective and that the potential for "chilling" effects exists, imposing a special relationship duty would not be justified.[193]

2. The Middle District of Florida's Analysis

The U.S. District Court for the Middle District of Florida also addressed the possibility of establishing a special relationship between a social media company and a user. *T.V. v. Grindr, LLC*[194] was brought on behalf of a minor, A.V., who allegedly used Grindr's services to engage in activities with adult users, resulting in emotional distress and bodily harm that culminated in A.V.'s suicide.[195] Grindr claims to be "the largest social networking app[] for gay, bi, trans, and queer people."[196] It publicizes the locations of its users on its platform and allows users to interact with the intention that the "chat may . . . lead to a date or sexual encounter."[197] Grindr also introduced "Grindr Tribes," which allowed users to identify with a niche group to filter their searches, which included the "Twink Tribe," which made minors feel welcome to download and use the app and allowed adult users to identify individuals under eighteen by narrowing their search results to the "Twink Tribe."[198] The presence of minors on the app created a niche market for Grindr that gave it an advantage over its competitors.[199] Moreover, Grindr knew that users under eighteen were especially vulnerable to physical danger by using its services, but failed to implement reasonable precautions to prevent underage users from accessing and subscribing to its services despite having the technology to do so.[200] One of the claims that T.V. brought was wrongful death based on negligence, contending that Grindr "owed a duty of care (negligence) to A.V. to exercise reasonable care to prevent foreseeable and known harms resulting from Grindr Services including . . . the online sexual grooming of children."[201] According to T.V., Grindr knew of the

192. Beckman v. Match.com, LLC, No. 13-CV-97, 2017 WL 1304288, at *3 (D. Nev. Mar. 10, 2017), *aff'd*, 743 F. App'x 142 (9th Cir. 2018).

193. Doe No. 14 v. Internet Brands, Inc., No. CV 12-3626, 2016 WL 11824793, at *5 (C.D. Cal. Nov. 14, 2016); *Dyroff*, 2017 WL 5665670, at *14.

194. No. 22-CV-864, 2024 WL 4128796 (M.D. Fla. Aug. 13, 2024).

195. *Id.* at *1.

196. *Id.* at *3 (alteration in original) (quoting Amended Complaint ¶ 12, T.V. v. Grindr, LLC, 2024 WL 4128796 (M.D. Fla. Aug. 13, 2024) (No. 22-CV-864)).

197. *Id.* (alterations in original) (quoting Amended Complaint ¶ 13, *Grindr*, 2024 WL 4128796 (No. 22-CV-864)).

198. *Id.* at *4.

199. *Id.*

200. *Id.* at *4–5.

201. *Id.* at *29 (alterations in original) (quoting Amended Complaint ¶¶ 97, 110, *Grindr*, 2024 WL 4128796 (No. 22-CV-864)).

potential dangers lurking on its site and that this was a viable basis for a duty to be found.[202]

At the motion to dismiss stage, the magistrate judge recommended that the plaintiff's duty of care claim proceed.[203] The court first clarified that "[a] court's decision as to whether a legal duty in negligence exists necessarily involves questions of public policy" and that Florida law applies a "foreseeable zone of risk" test to determine whether a duty of care exists.[204] This test draws from section 302B of the Restatement (Second) of Torts, that deems an act or omission to be negligent "if the actor realizes or should realize that it involves an unreasonable risk of harm to another through the conduct of the other or a third person which is intended to cause harm."[205] It was relevant that Grindr allegedly launched an app designed to facilitate the coupling of gay men, publicized users' locations, represented itself as a "safe space," created "Grindr Tribes" that made minors feel welcome and allowed users to more efficiently identify minor users, knew that minors were exposed to danger through the app, and had the ability to prevent minors from using Grindr but failed to take action.[206] The court viewed these allegations as creating a situation in which the actor (Grindr) would be required to anticipate and guard against the misconduct of others.[207] The court also found that some of the alleged conduct was affirmative in nature, rather than simple nonfeasance.[208] In addition, the court noted that public policy compelled a holding that the law entitles A.V. to protection because of the "vulnerabilities of the potential victims, the ubiquitousness of [social media], and the potential for extreme mental and physical suffering of minors."[209] The court analogized Grindr to a brick-and-mortar location, where there would be an obvious duty of care, and asserted that the fact of its virtual form should not affect that analysis.[210] The court did not opine on the existence of a special relationship, but found that Grindr's argument against it did not warrant dismissal because it failed to address the alternative basis for a duty of care based on its alleged affirmative acts that included introducing "Grindr Tribes."[211]

There are some notable distinctions in the duty analysis between *Grindr* and the three Ninth Circuit cases above. First, *Grindr* involved both

202. *Id.*
203. *Id.* at *37–38.
204. *Id.* at *35.
205. *Id.*; *see also* RESTATEMENT (SECOND) OF TORTS § 302B, cmt. f (AM. L. INST. 1965) ("Factors to be considered are the known character, past conduct, and tendencies of the person whose intentional conduct causes the harm, the temptation or opportunity which the situation may afford him for such misconduct, the gravity of the harm which may result, and the possibility that some other person will assume the responsibility for preventing the conduct or the harm, together with the burden of the precautions which the actor would be required to take.").
206. *Grindr*, 2024 WL 4128796, at *35.
207. *Id.*
208. *Id.*
209. *Id.* at *36.
210. *Id.*
211. *Id.*

misfeasance and nonfeasance by the social media company, and the court looked at an alternative avenue for finding a duty of care in the event that the plaintiff failed to allege sufficient facts to show a special relationship.[212] The magistrate judge's analysis in *Grindr* considered certain functionalities of Grindr to constitute affirmative acts, which diverges from the court's opinion in *Dyroff* which held that Ultimate Software's policy about anonymity and content-neutral tools did not show that Ultimate Software engaged in "substantial affirmative conduct . . . promoting the use of [the] tools for unlawful purposes."[213] The facts presented in *Grindr* did not indicate that the functions referenced only applied to select users, but that every Grindr user was able to take advantage of the "Tribes" and was subject to its geolocation feature. Second, in considering Grindr's affirmative acts and omissions, the court appeared to blend them together when listing what factors it found to be important for a duty of care analysis, whereas the California decisions firmly distinguished the two.[214] Third, the magistrate judge's analysis strayed from the Ninth Circuit's assessment of "custody or control" by dismissing Grindr's assertions that the complaint did not allege that Grindr had the ability to control its adult users nor identify how Grindr could have controlled the means through which they were accomplished.[215] Rather, the court found such a finding unnecessary because Florida's "foreseeable zone of risk" test does not require control over the instrumentality, premises, or person.[216] This test heavily emphasizes the factor of foreseeability, citing to *Demelus v. King Motor Co. of Fort Lauderdale*,[217] which noted that the Florida Supreme Court has significantly expanded the concept of duty in Florida negligence law and made foreseeability the sole determinant of whether a duty exists.[218] This is a large departure from the Central District of California's holding in *Internet Brands* that, despite the foreseeability that Flanders and Callum would commit more crimes through Model Mayhem, there was still no duty to warn.[219] However, the Middle District of Florida and the Ninth Circuit decisions were similar in considering whether policy justified a legal conclusion that the plaintiff was entitled to the defendant's protection.[220] Taken together, these cases

212. *Id.* at *35–36.

213. Dyroff v. Ultimate Software Grp., Inc., No. 17-CV-05359, 2017 WL 5665670, at *11 (N.D. Cal. Nov. 26, 2017), *aff'd*, 934 F.3d 1093 (9th Cir. 2019).

214. *See, e.g.*, Doe No. 14 v. Internet Brands, Inc., No. CV 12-3626, 2016 WL 11824793, at *4–5 (C.D. Cal. Nov. 14, 2016) (delineating between duties arising from misfeasance and nonfeasance); *see also* Dyroff v. Ultimate Software Grp., Inc., 934 F.3d 1093, 1100 (9th Cir. 2019) ("When analyzing a duty of care in the context of third-party acts, California courts distinguish between 'misfeasance' and 'nonfeasance.'").

215. *Grindr*, 2024 WL 4128796, at *36.

216. *Id.*

217. 24 So. 3d 759, 763 (Fla. Dist. Ct. App. 2009).

218. *Grindr*, 2024 WL 4128796, at *30.

219. *See Doe No. 14*, 2016 WL 11824793, at *5.

220. *See Grindr*, 2024 WL 4128796, at *36; *see also* Dyroff v. Ultimate Software Grp., Inc., No. 17-CV-05359, 2017 WL 5665670, at *12 (N.D. Cal. Nov. 26, 2017), *aff'd*, 934 F.3d 1093 (9th Cir. 2019).

illustrate how varied the legal analysis can be regarding the existence of a special relationship duty in social media cases.

B. Noninternet Special Relationship Cases

As the case law around this issue remains limited, courts assessing the question of whether a special relationship exists between social media platforms and users must turn to analogous cases that do not involve the internet.[221] This section will review a California case and a Florida case where courts have created a special relationship duty to identify the factors on which the courts have focused their analyses.

In *Safechuck v. MJJ Productions, Inc.*,[222] the California Court of Appeal was presented with the question of whether two corporations owned by Michael Jackson had a special relationship with the individuals who were allegedly sexually abused by Jackson while they were children.[223] The court found that the corporations had a special relationship to those individuals, stating that "a typical setting for the recognition of a special relationship is where 'the plaintiff is particularly vulnerable and dependent upon the defendant who, correspondingly, has some control over the plaintiff's welfare.'"[224] The plaintiffs' age at the time of the incidents was a critical factor to the court, because young children are recognized as being vulnerable and dependent on the protection of the adults who take care of them.[225] The children were often under the care and supervision of the defendants' employees, who organized and facilitated occasions for them to be alone with Jackson, knowing that Jackson might molest the children.[226] Thus, the court held that plaintiffs had every right to expect protection from the defendants because "[i]t is difficult to conceive a special relationship involving more foreseeable victims, or victims more dependent and vulnerable than these plaintiffs."[227] The court also emphasized the defendants' role in enabling Jackson to meet and be alone with the plaintiffs.[228] These factors insinuated that the defendants were best situated to prevent the alleged injuries.[229] The court was not persuaded by the defendants' argument that protective measures would have been impossible or absurd because Jackson, as their sole shareholder, would not have wanted

221. *See, e.g.*, *Doe No. 14*, 2016 WL 11824793, at *4 (citing *Conti v. Watchtower Bible & Tract Society of New York, Inc.*, 186 Cal. Rptr. 3d 26 (Ct. App. 2015), as a case with the most analogous facts).

222. 94 Cal. App. 5th 675 (Ct. App. 2023) (rehearing and review denied on September 6, 2023, and November 15, 2023, respectively).

223. *Id.* at 680–81.

224. *Id.* at 692 (quoting Brown v. USA Taekwondo, 483 P.3d 159, 169 (9th Cir. 2021)).

225. *Id.*

226. *Id.* at 692.

227. *Id.*

228. *Id.* ("Jackson did not meet the plaintiffs 'incidentally'; Jackson did not unwittingly 'stumble upon' them. Defendants employed both Jackson and the minor plaintiffs and made the arrangements enabling Jackson to be alone with them.").

229. *Id.* at 694.

to adopt them.[230] In his concurrence, Justice John Shepard Wiley Jr. wrote that "corporations cannot escape their tort duties by saying those with power do not care about safety. It is the job of tort law to make them care."[231]

In *Shurben v. Dollar Rent-a-Car*,[232] the Florida Third District Court of Appeal recognized a special relationship that requires a rental agency to warn a customer of foreseeable criminal conduct.[233] Patricia Ann Shurben was a British citizen who contacted a travel agent to purchase a vacation package to travel in Florida.[234] The travel package included a rental car provided by Dollar-Rent-a-Car ("Dollar") in Miami.[235] Although Shurben traveled in the rental car, which had a license plate specifically assigned to rental vehicles, from her hotel to a different part of Miami, she was accosted by unknown criminals and was shot in the struggle.[236] Shurben sued the car rental company, claiming that they breached their duty to warn her about parts of Miami where criminals targeted tourists in rental cars, particularly rental cars with the same license plate as hers.[237] She also alleged that Dollar was aware of prior similar attacks and knew that Shurben was a British tourist who did not know about the special license plate designation nor the crimes directed at tourists.[238] The court pointed to Dollar's superior knowledge to find that Dollar had a duty to warn Shurben of foreseeable criminal conduct.[239] The court thus held that a reasonable rental company in possession of such knowledge should understand that customers would be exposed to an unreasonable risk of harm if not warned and, therefore, had a duty to warn customers of the potential danger.[240]

The holdings in *Safechuck* and *Shurben* emphasized the plaintiffs' vulnerability, where certain characteristics, such as age and nationality, rendered the victims dependent on the defendants' protection or warning. The two courts also discussed how the defendants had actual knowledge of the risk, finding that their "superior knowledge" about hidden dangers placed them in the best position to protect the plaintiffs because they could foresee the harm occurring and possessed information that, if communicated to the potential victim, could avert that harm. For those reasons, the courts extended the special relationship doctrine to cover the above parties.

230. *Id.*
231. *Id.* at 705 (Wiley, J., concurring).
232. 676 So. 2d 467 (Fla. Dist. Ct. App. 1996).
233. *Id.* at 468.
234. *Id.* at 467.
235. *Id.*
236. *Id.*
237. *Id.* at 468.
238. *Id.*
239. *Id.*
240. *Id.*

III. COURTS SHOULD CONSIDER SUPERIOR KNOWLEDGE TO FIND A SPECIAL RELATIONSHIP BETWEEN SOCIAL MEDIA PLATFORMS AND THEIR USERS

This part calls for courts to expand the duty of care to social media cases in certain circumstances. Where the law permits a social media company to knowingly allow a vulnerable user to enter a dangerous situation that was facilitated through use of the social media platform, justice fails. Courts should recognize this inequity and aim to rectify it by finding that there is an affirmative duty on social media companies to warn their users about dangers of which they have actual or constructive knowledge of.

Part III.A discusses how public policy favors such an expansion, noting how the relationship between a social media company and its users is analogous to the special relationships in the Restatement (Second) of Torts, as well as the relatively minimal burden this would impose on social media companies. Then, Part III.B analyzes the *Internet Brands* case through the lens of a superior knowledge factor to demonstrate how incorporating that consideration leads to a more just resolution.

A. Public Policy Rationales for Expanding the Duty of Care

One of the guiding philosophies of American law is that it can react and conform to society's changing social, cultural, economic, and technological norms. It is also a basic tenet of tort law that for every wrong, there must be a right.[241] Thus, it is in the interest of public policy that courts be willing to reform their analyses of the special relationship doctrine as applied to internet providers to recognize the changing dynamics between social media companies and their users. In doing so, courts should consider whether a reasonable social media company, in possession of superior knowledge about hidden dangers on its site, should have realized that a failure to warn or protect would expose its users to an unreasonable risk of harm. If it does, courts should find that the plaintiff is entitled to protection, giving rise to a special relationship and duty to warn.

1. The Social Media-User Relationship Is Analogous to Established Special Relationships

The duty of an innkeeper to its guests is analogous to a situation where a social media company, through data mining or disclosure by a third party, acquires knowledge about a user's dangerous propensities and fails to warn other users who are likely to be harmed.[242] The question of custody and reliance is often where the special relationship argument fails, but to exercise custody means being in a position to control risks.[243] Social media

241. *See* Brodsky, *supra* note 16.

242. *See* Eyerman, *supra* note 109 and accompanying text.

243. *See* Banks v. Hyatt Corp., 722 F.2d 214, 225–26 (5th Cir. 1984); *see also* T.V. v. Grindr, LLC, No. 22-CV-864, 2024 WL 4128796, at *37 (M.D. Fla. Aug. 13, 2024).

companies have the ability to issue warnings and remove certain users, similar to how an innkeeper is able to warn guests about hidden dangers and drive out certain guests. In a situation where a natural person or a brick-and-mortar business would face liability, it is unreasonable for the law to permit a social media company to engage in the same behavior yet escape the consequences simply due to its online form, especially when issuing a warning would not impose an unfair burden on the company. Social media companies earn billions of dollars in revenue from their users and have the capacity and technology to issue these warnings.[244] Instagram's artificial intelligence warning system shows that the infrastructure and tools needed to quickly alert users of suspicious activity already exist and are used.

2. The Burden on Social Media Companies Does Not Outweigh the Benefits of Issuing Warnings

Social media companies should not be required to actively investigate users' backgrounds in greater depth than what is already being done. Instead, if the platform, in its ordinary course of business, discovers that one of its users poses a danger to other identifiable users, it should have a duty to warn those other users. The court in *Internet Brands* expressed concern that the efficacy of these warnings would be diluted if the company issued excessive amounts of warnings to avoid liability.[245] Though this may be true, the possibility that some users might disregard the warnings should not outweigh the potential for the warnings to protect other users, especially because doing so would only impose a minimal burden on the companies. This sentiment was shared by the court in *Tarasoff*, which held that the risk of giving unnecessary warnings is a reasonable price to pay for saving the lives of possible victims.[246] If the warnings could protect even a few users like Jane Doe or Mary Kay Beckman, that would be sufficient to justify them. Additionally, the law does not hold individuals liable for failing to actually protect someone; rather, it simply requires that certain individuals use reasonable care to inform authorities or warn potential victims.[247] Social media companies would not be under any obligation to conduct independent investigations into criminal issues, but, only to warn users of dangers they know or should have known about.[248] This further shows that a duty to warn would not be burdensome because it would not require social media companies to significantly modify their existing operations.

There are also concerns that creating such a requirement would circumvent § 230's protections.[249] However, the only instances where this special

244. *See supra* notes 27–30.

245. Doe No. 14 v. Internet Brands, Inc., No. CV 12-3626, 2016 WL 11824793, at *5 (C.D. Cal. Nov. 14, 2016).

246. Tarasoff v. Regents of Univ. of Cal., 551 P.2d 334, 346 (Cal. 1976).

247. *See id.* at 347.

248. *See* Shurben v. Dollar-Rent-a-Car, 676 So. 2d 467, 468 (Fla. Dist. Ct. App. 1996).

249. *See, e.g.*, Venkat Balasubramani, *9th Circuit Creates Problematic "Failure to Warn" Exception to Section 230 Immunity—Doe 14 v. Internet Brands*, TECH. & MKTG. L. BLOG

relationship duty to warn has been raised involved the social media company becoming aware of dangerous activity in a manner that was independent of the content itself.[250] Thus, creating a special relationship between social media companies and users would not seek to hold the companies liable as publishers of any third-party content. Additionally, finding that a special relationship exists between a social media company and its users would not open the floodgates of litigation because the plaintiff must still prove the other elements of negligence, and this duty to warn should be rooted in foreseeability and access to information unavailable to the plaintiff. Thus, if the social media company could not reasonably expect its users to meet in real life or if information about a dangerous user is readily available to the public, then the social media company would not face liability.

B. Applying a Superior Knowledge Factor to Internet Brands

In *Internet Brands*, Model Mayhem had been aware of the rape scheme for several years prior to Jane Doe's assault yet failed to warn her and other users about this danger.[251] This failure was especially egregious given that the company's business model was designed to facilitate networking within the modeling industry,[252] so the company could reasonably foresee that its users would eventually meet in real life. Thus, if the Ninth Circuit had included a factor like Florida's superior knowledge question in its special relationship analysis, Doe's case may not have been dismissed. Model Mayhem knew that its site was being used to perpetrate a rape scheme that was not disclosed to its users, knew that other users were likely to be harmed by the rape scheme, and should have known that its users would be exposed to an unreasonable risk of harm if not warned.[253] These facts make *Internet Brands* analogous to *Shurben*, where the Florida Third District Court of Appeal found a special relationship where the defendants possessed superior knowledge about foreseeable criminal conduct that the plaintiff did not have.[254] Such a factor would also be consistent with courts that recognize a *Tarasoff* duty to warn because that holding was premised on the idea that the law should require medical professionals to disclose potential dangers to reasonably identifiable third parties who may be injured if not warned.[255] Similar to the superior knowledge factor, *Tarasoff* references how doctors' medical expertise enables them to predict their patients' behavior.[256] This

(Sept. 23, 2014), https://blog.ericgoldman.org/archives/2014/09/9th-circuit-creates-problematic-failure-to-warn-exception-to-section-230-immunity-doe-v-internet-brands.htm [https://perma.cc/7JDZ-ZSAD].

250. *See supra* Part II.A.

251. Doe v. Internet Brands, Inc., 824 F.3d 846, 849 (9th Cir. 2016).

252. *Id.* at 848.

253. *See generally*, Doe No. 14 v. Internet Brands, Inc., No. CV 12-3626, 2016 WL 11824793, at *5 (C.D. Cal. Nov. 14, 2016).

254. Shurben v. Dollar-Rent-a-Car, 676 So. 2d 467, 468 (Fla. Dist. Ct. App. 1996).

255. Tarasoff v. Regents of Univ. of Cal., 551 P.2d 334, 347 (Cal. 1976).

256. *See id.* at 345.

should be viewed as analogous to how social media companies use data mining to predict their users' behaviors—thus putting them in a position of superior knowledge. It is unclear whether Model Mayhem utilized data mining, but it is not disputed that they had actual knowledge of the criminal activity that the plaintiff lacked. Had the Ninth Circuit considered Model Mayhem's superior knowledge, the court might have been more likely to find a special relationship between the website and Jane Doe, which would allow her to seek recovery against the website.

CONCLUSION

For better or for worse, technology and social media have transformed, and continue to transform, society. It is time that the law be reformed to impose responsibility on internet platforms commensurate with the large role they play in the daily lives of most Americans. Although courts have been reluctant to impose a duty of care on social media companies, this hesitation prevents victims like Jane Doe, Mary Kay Beckman, and Wesley Greer from obtaining recovery against companies profiting from their use that had actual or constructive knowledge of dangers that it could easily alert its users about. By adopting a superior knowledge factor into the special relationship analysis, plaintiffs will have a more viable claim against their wrongdoer. Moreover, recognizing a special relationship between social media companies and their users will result in more equitable outcomes without placing a large burden on the companies. Shifting the courts' perception of the legal role that social media holds in society is necessary to address modern internet issues. Social media has introduced a myriad of benefits, but it is also capable of facilitating immense harm. Therefore, the law must be equipped to reflect this and prioritize the safety of the human beings behind the screen.