Facebook, Defamation, and Terrorism: Who Is Responsible for Dangerous Posts on Social Media?

Caitlin McKeown*

I. INTRODUCTION

Technology and the Internet have created a whole new virtual world for the average person to explore. With the click of a button, people can share their thoughts, photos, and opinions, all while quickly analyzing information posted by other persons, news sites, companies, and politicians. While the Internet and social media have facilitated communication and opened the door to virtual exploration, there is an ever-growing trend towards threatened privacy and, even more serious, breaches in national security. Companies, like Facebook, have expanded beyond comprehension, with an average of 1.37 billion users active daily throughout the globe in June 2017 alone.[1] It is nearly impossible for Facebook and similar sites, such as Twitter, Google, and Myspace, to micromanage individual posts on such a massive, global scale. As a result, posts promulgating political insurgence, terrorism, and false,

* © 2017 Caitlin McKeown. J.D. candidate 2018, Tulane University Law School; B.A. 2013, The University of Chicago. I would like to thank my fellow members of the *Tulane Journal of International and Comparative Law* for all of their hard work and encouragement. In addition, I would like to dedicate my Comment to my parents, who have continuously shown their love and support throughout law school.

1. *Company Info*, FACEBOOK NEWSROOM, http://newsroom.fb.com/company-info/ (last visited Nov. 22, 2017).

incendiary data have plagued the Internet in recent years, bringing up the important question of who is responsible for this information and what avenues are available to stop it? Unfortunately, the answer still remains unclear in both the United States and abroad.

In the United States, this question is coupled with an analysis of Free Speech under the Constitution, as well as a federal immunity statute known as the Communications Decency Act (CDA), which removes liability from online publishers for defamatory or incendiary posts made by third party users.[2] In the past year, a variety of lawsuits have been filed against tech giants, like Facebook and Twitter, under §§ 2339A and 2339B of the Patriot Act, better known as the Material Support Statute.[3] This statute has been clashing with the CDA, when families of terrorist victims sue these corporate giants in the hopes of placing liability on websites for disseminating terrorist propaganda, albeit unknowingly, through their websites.[4] However, courts have been wary to accept these material support arguments, continuing to favor immunity for corporations as mere publishers of the content.[5]

This Comment will examine the origins of CDA in the United States alongside developments in antiterrorism legislation, including the Material Support Statute of the U.S. Patriot Act, and its application to social media. Specifically, it will analyze the two statutes in detail and delve into a discussion of how plaintiffs in antiterrorism legislation are finding new ways to sue Internet sites under the Material Support Statute, as well as how these websites are rebutting such claims by invoking the long-standing immunity of the CDA. Furthermore, this Comment will examine potential loopholes around the CDA via suggested changes to both the statute and case law, including the idea of making websites liable for dangerous content via site-wide report and remove systems, potential amendments to the CDA, and by applying more plaintiff friendly case precedent as seen in the Ninth Circuit.[6] Finally, this Comment will examine similar types of litigation abroad, specifically a German case filed by a Syrian refugee whose "selfie" with Chancellor Angela Merkel led to an onslaught of false posts and

---

2. 47 U.S.C. § 230 (1998).
3. *See* 18 U.S.C. § 2339A (2009); *see also* 18 U.S.C. § 2339B (2015).
4. *See* 47 U.S.C. § 230 (1998).
5. *See generally* Blumenthal v. Drudge, 992 F. Supp. 44, 52 (D.C. Cir. 1998).
6. *See* Michael Burke, *Cracks in the Armor?: The Future of the Communications Decency Act and Potential Challenges to the Protections of Section 230 to Gossip Web Sites*, 17 B.U. J. SCI. & TECH. L. 232, 257-58 (2011); *see also* Patricia Spiccia, *The Best Things in Life Are Not Free: Why Immunity Under Section 230 of the Communications Decency Act Should Be Earned and Not Freely Given*, 48 VAL. U. L. REV. 369, 408-16 (2013).

photoshopped images of the refugee on Facebook terrorist propaganda pages.[7] The importance of this decision abroad is that it showcases that these types of issues are not localized to one country or continent but are concerns that need to be addressed and resolved on a global scale with the assistance of worldwide corporate tech giants, like Facebook, Google, and Twitter. Companies, like Facebook, by enacting uniform corporate policy to combat online terrorism and defamation, might be the first step in encouraging countries to amend their laws and promote more consumer-oriented judicial recourse when it comes to the Internet.

II. BACKGROUND

A. The Communications Decency Act—Origins and History

Before delving into recent antiterrorist and antidefamation case law under the Material Support Statute and online publisher immunity, it is important to understand the background and fundamental underpinnings of the CDA. In 1996, the U.S. Congress created the CDA to combat quickly amassing concerns regarding the ability of young children to view pornography and other offensive material on the Internet.[8] The CDA stated that it was punishable under criminal law to "knowingly transmit 'obscene' or 'indecent' messages, as determined by local community standards" to a minor and "prohibited knowingly sending or displaying a 'patently offensive' message containing sexual or excretory activities . . . to a minor."[9] While the general language of the CDA imposed a broad ban on certain materials, it did provide an effective loophole with what is known as the good faith clause.[10] Essentially, the good faith clause stated that if an individual or website took obvious

---

7. *See* Melissa Eddy, *How a Refugee's Selfie with Merkel Led to a Facebook Lawsuit*, N.Y. TIMES (Feb. 6, 2017), https://www.nytimes.com/2017/02/06/business/syria-refugee-anas-modamani-germany-facebook.html?_r=0.

8. *See* Telecommunications Act of 1996, Pub. L. 104–104, 110 Stat. 56, Title V, § 502 (1996).

9. William A. Sodeman, *Communications Decency Act (CDA) United States [1996]*, ENCYCLOPEDIA BRITANNICA (Nov. 24, 2016), https://www.britannica.com/topic/Communications-Decency-Act.

10. *Id.*; *see also* Telecommunications Act of 1996 § 502(d)(5)(A)-(B), which specifically states:

> [I]it is a defense to a prosecution under [the Act] . . . [if] a person (A) has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology; or (B) has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.

efforts to prevent children from accessing inappropriate materials on their site, they may have an adequate defense in court.[11]

While the CDA's purpose may have been noble, courts were greeted by a plethora of lawsuits challenging the statute's abstruse language. Obscurity regarding the good faith exception was a major point of contention, with Internet service providers (ISPs) unsure of how to effectively weed out minor users from their websites without alienating older, consenting users.[12] Secondly, the language of the CDA was extremely broad, making it nearly impossible to define what material fell within the definition of "indecent" or "patently offensive" under the statute's own language.[13] ISPs argued that these blanket statements violated the First Amendment by placing an enormously difficult task on Internet providers to censor content with no rational definitions or guidelines.[14] Finally, issues arose concerning the statute's phrase "contemporary community standards," which ISPs were expected to use as a pathway for determining those materials that were offensive from those that were not.[15] This was an obvious issue as different states have varying local standards that are used, making the statute lack any sort of uniformity or general guidance.[16]

A landmark case, *Reno v. ACLU*, changed the scope of the CDA and helped formulate the standards for § 230 that are currently in use today.[17] In *Reno v. ACLU*, a variety of ISPs filed a lawsuit against the Attorney General and the Department of Justice challenging the statute's constitutionality under the First Amendment, particularly due to the statute's confusing use of the language "indecent" and "patently offensive."[18] The Supreme Court found the CDA to be unconstitutional because it was far-reaching and too limiting, resulting in a violation of free speech.[19] The Court examined the statute's language, including the provisions regarding "indecent" and "patently offensive" materials, and found that:

---

11. Sodeman, *supra* note 9.

12. *Id.* As stated within the CDA *Britannica* article, some ISPs used the suggested credit card and age verifications as a method of removing minors from their sites to invoke the good faith exception. *Id.* However, ISPs were wary of this as it had the potential to harm their business with adults. *Id.*

13. *Id.*; *see also* Telecommunications Act of 1996 § 502(a).

14. Sodeman, *supra* note 9.

15. *Id.*; Telecommunications Act of 1996 § 502(d)(1)(B).

16. Sodeman, *supra* note 9.

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

18. *Id.*

19. *Id.* at 874-75.

> [T]he CDA lacks the precision that the First Amendment requires when a statute regulates the content of a speech. In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.[20]

In conclusion, the Court found that the CDA did more to hinder free speech on the Internet rather than to encourage it.[21] This prompted the statute to be revised, and for the term "indecent" to be officially removed from the language of the CDA.[22]

It is important to note that while the Supreme Court found the CDA to be unconstitutional for its broad prohibition on obscene materials in light of free speech, the CDA does still uphold the idea that online defamation is illegal and punishable by law.[23] This portion of the CDA survived the Supreme Court's gutting of the statute, and most online defamation claims are governed under its scope. However, the modern § 230 makes a clear distinction for third party ISPs in defamation claims, a source of major contention in recent lawsuits addressing issues of individual privacy and national security online.

B. The Modern CDA—§ 230 and Publisher Immunity

The most important section of the modern CDA is § 230(c)(1), otherwise known as the publisher immunity clause.[24] Section 230(c)(1) states that "no provider or user of interactive computer service shall be treated as the publisher or speaker of information provided by another information content provider."[25] This statement removes liability from publishers of false, dangerous, or misleading content online.[26] Furthermore, the immunity granted under § 230(c)(1) is subject to the Supremacy Clause, meaning that it trumps all state and local legislation that might oppose it.[27] It is also important to note that an ISP is not required to remove any false information posted throughout its website,

---

20. *Id.*
21. *Id.*
22. *Id.*
23. *The Communications Decency Act and Its Effect on Online Libel*, REPUTATION HAWK, https://www.reputationhawk.com/communicationsdecencyact.html (last visited Mar. 21, 2016).
24. *See* 47 U.S.C. § 230(c)(1) (1998).
25. *Id.*
26. Timothy L. Alger, *The Communications Decency Act: Making Sense of the Federal Immunity for Online Services*, 59 ORANGE COUNTY L. 30, 31 (2017).
27. *Id.*

even when the provider is put on notice that the content exists.[28] While the CDA does not prohibit all types of civil and criminal claims, it has opened the door for ISPs, allowing for the unprecedented growth of social media sites and search engines largely unhindered by any sort of regulation or responsibility for the content posted throughout their websites.[29]

When discussing the CDA, it is important to learn the distinction between interactive computer services (ICS) and information content providers (ICP) as these have very different implications under the CDA's scheme.[30] While both fall under the general definition of an ISP, they do have distinct differences. An ICS is "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server."[31] It is widely accepted that search engines, like Google, and social media sites, like Facebook and Twitter, fall under the statute's definition of an ICS.[32] In contrast, an ICP is "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[33] Essentially, the difference is that the former is the site allowing access to the data by providing the Internet platform only, while the latter is responsible for the actual information being created *and* distributed. This would mean that ICPs are not granted federal immunity under the CDA like ICSs.[34]

The first major case to address publisher immunity under the CDA, and the case that set the precedent for CDA litigation for many years, was *Zeran v. America Online, Inc.* in the U.S. Fourth Circuit Court of Appeals.[35] In *Zeran*, a man sued AOL for negligence when he received an array of death threats after an unidentified user falsely linked his phone number to the sale of offensive apparel relating to the Oklahoma City bombing.[36] The t-shirts and accessories in question were posted for sale via an AOL bulletin board, where Zeran's phone number was linked as the contact for sales.[37] The post resulted in the local newspaper and local radio shows condemning the apparel and encouraging readers and

---

28. *Id.*
29. *Id.* at 31-32.
30. *Id.* at 31; *see also* Spiccia, *supra* note 6, at 385-86.
31. 47 U.S.C. § 230(f)(2) (1998).
32. Alger, *supra* note 26, at 31.
33. 47 U.S.C. § 230 (f)(3).
34. Alger, *supra* note 26, at 33.
35. *See* Zeran v. Am. Online, Inc., 129 F.3d 328, 329 (4th. Cir. 1997).
36. *Id.*
37. *Id.*

listeners to bombard the listed phone number to voice their complaints.[38] After receiving hundreds of threatening phone calls, Zeran repeatedly contacted AOL to insist that the post be removed, but to no avail.[39] Zeran then sued, stating that AOL was negligent in failing to promptly remove the content, for failing to post any sort of response to the posts, and for declining to implement any sort of screening process.[40] The court held that the purpose of § 230 was to prevent government regulation and intrusion into the realm of online free speech.[41] The court further held that while "the original culpable party who posts defamatory messages would [not] escape accountability . . . Congress made a policy choice . . . not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages."[42] Furthermore, the court found that AOL's "[decision] whether to publish, edit, or withdraw user content" was specifically the duty of a publisher under the CDA.[43] The court also acknowledged the sheer impracticability, nay impossibility, that Internet providers can monitor millions of posts for potential defamation.[44] The court found that implementing such restrictive policies and regulations was counterintuitive to the CDA's purpose and would merely result in a restriction of free speech.[45] Therefore, the Fourth Circuit laid out the precedent that the CDA immunized a large array of websites that display defamatory content, all while eliminating responsibility for removing, editing, or combating such material by labeling them as publishers for purposes of the statute.[46]

The *Zeran* decision has dictated CDA case law for decades, with courts broadening the scope of publisher immunity even further.[47] For example, in a major Fifth Circuit case, *Doe v. MySpace*, the court rejected the plaintiff's argument that her thirteen-year-old daughter would not have been assaulted due to an online post asking to contact her and meet her in person, if MySpace had taken preventative measures to ensure that the users posting on the site were adults.[48] The court, once again, held MySpace as immune under the CDA for the publication of

38. *Id.*
39. *Id.*
40. *Id.* at 328.
41. *Id.*
42. *Id.* at 330-31.
43. *Id.* at 332-33.
44. *Id.* at 330-31.
45. *Id.* at 331.
46. *Id.*
47. *Id.*
48. Doe v. MySpace, Inc., 528 F.3d 415, 416 (5th Cir. 2008).

third party content, with the plaintiff's recourse being to sue the third party posters themselves.[49] The court in another famous case, *Blumenthal v. Drudge*, found that even though the ISP in question maintained minor editorial control over the published content, the defendant ISP was still immune under § 230.[50] In *Blumenthal*, the plaintiffs sued Drudge and AOL for a gossip column Drudge wrote and dispensed through AOL's services.[51] The court found that while Drudge was responsible for writing the content, AOL remained immune from the suit as the publisher of the information, even when it held certain "editorial rights with respect to the content provided by Drudge and disseminated by AOL, including the right to require changes in content and to remove it."[52] As such, the court upheld the idea that an ISP can hold some editorial qualities while still maintaining its immune status under the CDA.[53] In summation, CDA immunity has been condensed through years of litigation into specific categories that create a high bar for any plaintiff to reach to prove liability against ISPs in civil suits.[54]

While efforts to combat the CDA's publisher immunity clause seemed futile throughout the 1990s and early 2000s, recent developments in the Ninth Circuit have provided hope for plaintiffs in cases involving online defamation and predation.[55] In 2008, the Ninth Circuit created a loophole around CDA immunity for ISPs by supporting a claim of promissory estoppel in *Barnes v. Yahoo!, Inc.*[56] Barnes filed suit against Yahoo when she repeatedly requested that Yahoo remove pornographic photos of herself posted by her ex-boyfriend in Yahoo chatrooms.[57] After many attempts to get the photos removed, Yahoo responded that it was in

---

49. *Id.* at 420-22.
50. *See* Blumenthal v. Drudge, 992 F. Supp. 44, 52 (D.C. Cir. 1998).
51. *Id.* at 46-48.
52. *Id.* at 51.
53. *Id.*
54. *See* KATHLEEN ANN RUANE, CONG. RESEARCH SERV., R44626, THE ADVOCACY OF TERRORISM ON THE INTERNET: FREEDOM OF SPEECH ISSUES AND THE MATERIAL SUPPORT STATUTES 21-22 (2016). Ruane nicely sums up the major subcategories of CDA litigation into a three-part test. *Id.* She states:

> [A] three-part test has been developed to determine whether a defendant is eligible for Section 230's protection. If the lawsuit is: 1. Brought against [an] interactive computer service provider or user (e.g., a website like NYTimes.com, or a social media service like Twitter or Facebook), 2. Based upon information provided by another content provider, and 3. Seeks to hold the defendant liable as a publisher or speaker of that content, then Section 230's liability shield applies.

Id.

55. *See,* e.g., Barnes v. Yahoo!, Inc., 570 F.3d 1098, 1109 (9th Cir. 2009).
56. *See id.* at 1109.
57. *Id.* at 1098-99.

the process of stopping the unauthorized posts.[58] The posts continued until Barnes filed suit, at which point the profiles disappeared.[59] While the court reasoned that Yahoo escaped liability on the basis of the content as a publisher under the CDA, the court did uphold the plaintiff's claim of promissory estoppel in that she relied on Yahoo's promise to remove the inappropriate content.[60] The court found that "the promise created a duty independent of the tort rules controlling publishers, as well as Section 230(c)(1) immunity."[61]

In a recent decision from 2016, *Jane Doe v. Internet Brands, Inc.*, the Ninth Circuit reversed the district court's dismissal of an aspiring model's claim against the site, Model Mayhem, for negligent failure to warn after she was lured to a fake audition posted on the website and assaulted.[62] While the court upheld that Internet Brands was an ICS that is technically immune under § 230, the suit, here, was about the site's failure to warn models about the information it retrieved from unknown sources.[63] Specifically, the court found that "the duty to warn allegedly imposed by California law would not require Internet Brands to remove any user content or otherwise affect how it publishes or monitors such content."[64] Because this claim was removed from the defendant's identity as an online publisher, it was not barred under the CDA.[65]

Finally, an important decision in the Ninth Circuit from 2008 deviates from the idea of providing absolute immunity to ISPs when they "materially contribute" to the unlawful content posted on their website.[66] In *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, the Ninth Circuit found that the defendant could not escape liability under the CDA when it "contributes materially to the alleged illegality of the conduct."[67] The Fair Housing Council brought suit against Roommates.com, a website that matched available apartments to renters, alleging that the website violated the Fair Housing Act and housing discrimination laws via a requirement that renters fill out a profile describing their sexual orientation, gender, and other personal

58. *Id.*
59. *Id.*
60. *Id.* at 1108-09.
61. Alger, *supra* note 26, at 32-33.
62. *See* Jane Doe No. 14 v. Internet Brands, Inc., 824 F.3d 848, 848 (9th Cir. 2016).
63. *Id.* at 851.
64. *Id.*
65. *Id.*
66. Alger, *supra* note 26, at 34; *see* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1161, 1175 (9th Cir. 2008).
67. *Fair Hous.*, 521 F.3d at 1168.

information.[68] This created *de facto* discrimination by filtering and limiting the number of listings that users saw based on the personal information provided.[69] The court found that while federal immunity under the CDA does remain in place for ISPs and similar websites, this immunity should be foregone when the website encourages the illicit content through its own actions.[70] Here, Roommates.com actively encouraged discrimination in direct contravention to state and local fair housing laws and, in essence, was directly associated with the illegality of the site.[71] More specifically, the court stated that "the message to website operators is clear: if you don't encourage illegal content, or design your website to require users to input illegal content, you will be immune."[72] This case is a landmark for CDA litigation and provides a potential loophole for litigants in cases involving illegal online activity. If plaintiffs are able to prove that the website in question had a specific role in forcing or requiring users into engaging with some sort of illicit activity, the CDA's immunity could potentially be bypassed.[73] However, it should be noted that in the years following the *Roommates.com* decision, courts have been wary to accept the court's analysis, deeming it an unusual case based around a rare, specific set of facts—i.e., in order to use the site users *had* to post facially illegal information.[74] Courts have expanded on the *Roommates.com* ruling finding that "while requiring users to engage in illegality might defeat the immunity, encouraging or even endorsing allegedly defamatory statements by users probably does not."[75] While this case is a strong exception to the CDA's immunity, it is an incredibly high threshold to meet.[76] Even so, these decisions, coupled with an increasing awareness of § 230 and activities conducted online, could provide effective loopholes around publisher immunity in cases involving defamation and criminal activity on the Internet. More importantly, this may be an effective route for plaintiffs to follow in litigation involving terrorist organizations and material contributions to terrorist-funded groups via online networks.

---

68. *Id.* at 1161-62.
69. *Id.*
70. *Id.* at 1174-75.
71. *Id.*
72. *Id.* at 1175.
73. *Id.*
74. Alger, *supra* note 26, at 35.
75. *Id.*
76. *Id.*

C. The Material Support Statute and Its Connection to Terrorism Online

The Material Support Statute has come into the spotlight recently due to an increasing number of cases filed in the wake of modern terrorist attacks invoking the statute. These lawsuits are centered around the idea that while it is difficult to pinpoint directly who is fully involved in, and responsible for, acts of terror committed both domestically and abroad, some liability should fall onto major web-based companies who allow certain terrorist funded profiles and webpages to be created and remain unmonitored on their platforms.[77] First, it is necessary to discuss the foundation of the Material Support Statute and what its main purpose is in conjunction with terrorism. Second, it is important to discuss the historical case precedent surrounding the statute and address the question of what constitutes material support for terrorism, both on and offline, under the U.S. Constitution.

Created in the mid-1990s as part of the Patriot Act, 18 U.S.C. § 2339A and § 2339B are central to combating terrorism both abroad and on U.S. soil.[78] Section 2339A specifically prohibits "support[ing] or concealing support for the crimes a terrorist has committed or may be planning to commit."[79] Section 2339B is a little more specific in that it "condemns providing material support to foreign terrorist organizations that engage in such offenses."[80] This directly correlates to terrorist groups that are already known, e.g., Al Qaeda, Hamas, and ISIS, while § 2339A connects to issues that involve terrorism in a more general sense.[81] Material support is a relatively broad and inclusive term, including both tangible and intangible goods.[82] This means that material support can be in the form of written or oral guidance, as well as something like physical currency, weapons, or transportation.[83] These charges are serious, resulting in imprisonment ranging from fifteen to twenty years along with steep fines ranging up to half a million dollars for the most serious offenses.[84] It is important to note that these are federal, criminal offenses, and no civil causes of action may arise from

---

77. *See generally* Fields v. Twitter, Inc., No. 16-CV-00213-WHO, 2016 WL 6822065 *1 (N.D. Cal. Nov. 18, 2016).

78. *See* CHARLES DOYLE, CONG. RESEARCH SERV., R41333, TERRORIST MATERIAL SUPPORT: AN OVERVIEW OF 18 U.S.C § 2339A AND § 2339B 1 (2016).

79. *Id.* at 2; *see* 18 U.S.C. § 2339A (2009).

80. DOYLE, *supra* note 77, at 13; *see* 18 U.S.C. § 2339B (2015).

81. DOYLE, *supra* note 77, at 13.

82. *Id.* at 13, 17.

83. *Id.* at 8, 16.

84. *Id.* at 9, 20.

violations of the Material Support Statute.[85] However, 18 U.S.C. § 2333 permits U.S. citizens harmed by terrorism abroad to collect damages under §§ 2339A and 2339B.[86]

While sensible in its goals, the material support statute was met with an onslaught of litigation questioning the statute's definitions of what exactly constituted material support under the Constitution.[87] In the famous case, *Holder v. Humanitarian Law Project*, the Supreme Court decided the fate of interpreting the Material Support Statute and held that the statute's provisions were not in violation of the First Amendment.[88] In *Holder*, the plaintiffs contested the constitutionality of the Material Support Statute, holding that their active support for the peaceful features of the Kurdistan Workers' Party and the Liberation Tigers of Tamil Eelam, both documented terrorist organizations under § 2339B, violated their right of free speech and association under the First Amendment.[89] The plaintiffs, consisting of U.S. citizens and organizations, argued that they wished to support the "humanitarian and political activities" of the two groups via donations, education, and "political advocacy," despite the organizations' involvement in terrorist attacks that killed numerous American citizens.[90] The crux of the plaintiffs' argument rested on the fact that they wished to provide material support to the peaceful parts of the two terrorist groups, making a blanket ban on all of these activities unconstitutional.[91] In further contravention to the plaintiffs' argument, Congress amended the statute in 2001 redefining material support to include "expert advice or assistance."[92]

The Court found that the statute was not overly vague and in violation of the Constitution like the plaintiffs contended, holding that providing material support in the form of "training," "expert advice or assistance," "service," or "personnel" could all be barred in conjunction with terrorist organizations under the Constitution.[93] The Court also held that the statute "'does not prohibit independent advocacy or expression of any kind . . . [and] does not prevent [plaintiffs] from becoming members of [the organizations] or impose any sanction on them for

85. *Id.* at 23.
86. RUANE, *supra* note 54, at 20.
87. *See, e.g.*, Holder v. Humanitarian Law Project, 130 S. Ct. 2712, 2712 (2010).
88. Holder v. Humanitarian Law Project, 130 S. Ct. 2712, 2712 (2010).
89. *Id.* at 2713.
90. *Id.* at 2714-15.
91. *Id.* at 2715.
92. *Id.*
93. *Id.* at 2722-29.

doing so.'"[94] Instead, the statute limits the plaintiffs' ability to provide support, whether it is tangible, like monetary contributions, or intangible, like training and education via verbal communications.[95] Essentially, the Court reasoned that speech that provides sensitive information, specific knowledge, or trains someone in a specific skill furthers terrorism in this type of scenario.[96]

The *Holder* decision has been widely criticized by activist groups and politicians alike, who argue that the decision's severe attitude towards most types of generalized assistance and educational training services with these types of groups is harmful towards citizens directly affected by foreign conflicts, who usually seek out these organizations for shelter and aid.[97] Many also argue that it disrupts potential peace discussions by limiting most types of beneficial contact with U.S. designated terrorist groups.[98] In the years following the *Holder* decision, the rise of the Internet has made it exceptionally simple for terrorist organizations to disseminate information and garner support for their organizations through the web.[99] A lack of Internet background checks on social media sites have led terrorist organizations to create various profiles on pages throughout Twitter and Facebook, with a recent study producing data that ISIS controlled approximately 30,000 Twitter accounts in 2014.[100] In light of these recent events, legal scholars have begun to wonder whether providing social media accounts to terrorists, like those provided via Facebook and Twitter, should constitute a violation of § 2339B.[101] Furthermore, the issue behind suing a social media giant in connection with § 2339B of the material support statute is the requirement that the site has requisite knowledge or some kind of role in the organization and its illegal and/or violent activities, as well as direct contact with the terrorist organization itself in the formation of the webpage or online profile.[102] Naturally, given the massive scale of Internet sites, like Facebook and Twitter, courts have remained more lenient towards online service providers in this context because of the difficulty, nay

94. *Id.* at 2730.
95. *Id.*
96. *Id.* at 2743.
97. *See* Adam Liptak, *Court Affirms Ban on Aiding Groups Tied to Terror*, N.Y. TIMES (June 21, 2010), http://www.nytimes.com/2010/06/22/us/politics/22scotus.html.
98. *Id.*
99. RUANE, *supra* note 54, at 17.
100. *Id.*
101. *Id.*
102. *Id.* at 18-20.

impossibility, these companies would face in monitoring each and every profile created on their websites.[103]

Despite the difficulties plaintiffs would face in these legal scenarios, a number of lawsuits have been filed over the past two years demanding that sites, such as Twitter, Facebook, YouTube, and Google, take responsibility for acts of terror in the United States and abroad.[104] The crux of these arguments is that the sites are providing, via nonaction and implicit consent, material support to terrorist organizations.[105] These cases, explored in the next Part, are combining the legal arguments behind the Material Support Statute and the CDA in an attempt to place more responsibility, and liability, on social media sites for acts of terror and violence committed both domestically and abroad.

III. TERRORISM AND SOCIAL MEDIA—A NEW FRONTIER UNDER THE CDA AND § 2339B

Three major statutory regimes come into play for plaintiffs filing lawsuits against social media giants under the Material Support Statute in relation to terrorist materials disseminated online: The Anti-Terrorism Act, the Material Support Statute, and the CDA.[106] Under 18 U.S.C. § 2333, or the Anti-Terrorism Act, American citizens and their families may recover damages in a private civil lawsuit for any injury to "[their] person, property, or business by reason of an act of international terrorism."[107] This incorporates § 2339A and § 2339B, which courts have held to involve international acts of terrorism.[108] Therefore, plaintiffs may invoke the Material Support Statute in a civil suit for damages against entities for online posts in connection to acts of terror. However, this argument will only succeed if the entity in question is involved in the creation of the online content and is not merely the publisher of the information, falling outside the liability exception of the CDA.[109]

A case filed in California in 2016 has attempted to combat international terrorism by arguing that culpability and liability should be placed on Internet providers, such as Twitter, Facebook YouTube, and Google, for terrorist attacks organized via the Internet that resulted in

---

103. *Id.*

104. *See, e.g.*, Fields v. Twitter, Inc., No. 16-CV-00213-WHO, 2016 WL 6822065, at *1 (N.D. Cal. Nov. 18, 2016).

105. *Id.*

106. *See* 18 U.S.C. § 2333 (2009); 18 U.S.C. § 2339A (2009); 18 U.S.C. § 2339B (2015); 47 U.S.C. § 230 (1998).

107. *See* 18 U.S.C. § 2333(a) (2016).

108. RUANE, *supra* note 54, at 20.

109. *See generally* Blumenthal v. Drudge, 992 F. Supp. 44, 52 (D.C. Cir. 1998).

injuries to U.S. citizens.[110] The recent decision in *Fields v. Twitter* has shed some light on the potential avenues for legal recompense for victims of terrorism and has also highlighted just how broad the CDA's interpretation and publisher immunity extends.[111]

In *Fields*, the widows of U.S. contractors killed in Amman, Jordan, during an ISIS attack, brought suit against Twitter, alleging that Twitter had provided material support to ISIS under § 2339B by giving them Twitter accounts, and that these accounts were generally linked to their husbands' deaths abroad.[112] More specifically, Fields and Creach were government contractors who were assigned to the International Police Training Center in Amman, Jordan, when Anwar Abu Zaid, a Jordanian police captain, snuck an assault rifle and other weapons into the center killing the two men.[113] Following the attack, ISIS claimed responsibility for the deaths, acknowledging that the attack was planned.[114] The widows of the contractors brought suit against Twitter in a fairly unique way. They did not allege that Twitter was directly involved in the attack via recruitment or communication with ISIS leaders, nor did they allege that ISIS members even viewed these ISIS propaganda Twitter accounts prior to the attack.[115] Instead, they raised the argument that Twitter violated §§ 2339A and 2339B, vis-à-vis § 2333 of the Anti-Terrorism Act, by knowingly contributing material support to ISIS and other terrorist organizations online.[116] They argued that Twitter, by allowing ISIS sponsored profiles to exist and distribute information on its website, aided and facilitated the terrorist attacks in Jordan and directly related to the deaths of the American contractors in Amman.[117] The lawsuit, in essence, stated that while ISIS may not have directly recruited Abu Zaid via Twitter, nor directly organized the attack via Twitter, "the attacker was generally inspired by propaganda that he had seen on Twitter," creating an overarching link between the website and the ISIS attacks.[118]

Twitter launched an obvious counterattack to the widows' argument by invoking § 230 of the CDA, claiming that because they were merely a publisher of online information, and not the direct contributor of the

---

110. Fields v. Twitter, Inc., No. 16-CV-00213-WHO, 2016 WL 6822065, at *1 (N.D. Cal. Nov. 18, 2016).

111. RUANE, *supra* note 54, at 22; *see also Fields*, 2016 WL 6822065, at *1.

112. *See Fields*, 2016 WL 6822065, at *1.

113. *Id.*

114. *Id.*

115. *Id.* at *2.

116. *Id.* at *1-2.

117. *Id.*

118. RUANE, *supra* note 54, at 22.

content itself, they were immune under the statute and could not be held liable in relation to a federal, criminal offense, such as those punishable under §§ 2339A and 2339B.[119] The plaintiffs had two major arguments that they presented in response to Twitter's claims of immunity.[120] First, the plaintiffs argued that content was not the issue in this scenario but rather Twitter's "provision of services" and the profiles that were freely given to ISIS.[121] Second, they invoked the "direct messaging service" that Twitter offered, arguing that these private messages do not amount to published materials, removing immunity from these types of communications under § 230.[122] The court rejected both of these arguments using prior § 230 case law that discussed the broad application that the statute provided for third party content on a website, such as Twitter.[123] The court, invoking case law from the Ninth Circuit, also found that Twitter's decision to grant accounts to particular individuals for the purposes of posting content, as well as removing the content should Twitter see fit, related to their role as a publisher—even if the accounts in question involved ISIS.[124] Furthermore, the court was not convinced by the plaintiffs' argument regarding private messaging.[125] The court turned to precedent to determine that "in defamation law, the term 'publication' means 'communication [of the defamatory matter] intentionally or by a negligent act to one other than the person defamed.'"[126] Applying this definition, the court found that Twitter was still only a publisher of the information conveyed via direct messages, because whether or not the information was made publicly available was non-consequential to Twitter's role as an ICS.[127] In conclusion, the court held that Twitter, even in providing accounts to ISIS agents and permitting private messaging through its direct messaging service, was still merely acting in its role as a publisher and was immune from liability for acts of terror committed abroad.[128]

In the wake of the *Fields* case, a variety of other lawsuits, alleging similar arguments and facts, have been brought against online companies, including YouTube, Google, Twitter, and Facebook. Another

119. *Fields*, 2016 WL 6822065, at *3-5.
120. *Id.* at *5.
121. *Id.*
122. *Id.* at *5-10; *see also* RUANE, *supra* note 54, at 23.
123. *Fields*, 2016 WL 6822065, at *5-10.
124. *Id.*
125. *Id.* at *10-11.
126. *Id.* at *10.
127. *Id.* at *10-11.
128. *Id.*

lawsuit was filed in the Northern District of California by the father of one of the victim's killed in the Paris attacks in 2015.[129] That lawsuit similarly alleged violations of the Material Support Statute, met by vehement denials of involvement from Twitter, Facebook, and Google, as well as a request for dismissal under the CDA's publisher immunity clause.[130] On top of publisher immunity, these sites are also invoking their disclaimers, stating that sites, like Facebook and Twitter, have prominent anti-violence and antiterrorism rules in connection to their platforms.[131] However, critics of the websites state that while these rules may be listed, little is done about enforcing them, despite much of the power about what content and users should be removed remaining with the sites themselves.[132] Another lawsuit was filed against Twitter, Google, and Facebook this past December by family members of victims of the Pulse nightclub shooting in Orlando, Florida, alleging that the companies "'knowingly and recklessly' provid[ed] ISIS with user accounts 'as a tool for spreading extremist propaganda, raising funds, and attracting new recruits.'"[133]

What these cases have displayed is that while it is in the country's interest to ensure that the families of victims of terrorist attacks in both the United States and abroad have proper channels to receive compensation for such tragedies, it is difficult to say that an amendment of the CDA that generally pushes liability onto websites would enact positive change or stop terrorism's facilitation through the Internet. The connection that these websites have to terrorist organizations is tenuous, with their sites only acting as a platform for third parties to provide content wholly separate from the company and its employees. While it is attractive to sue websites, like Facebook, in connection to such attacks domestically and abroad, where other potential defendants may be unknown or impossible to sue, it is quite probable that allowing such claims to succeed in court could leave devastating effects on Internet providers and would open the door to claims beyond terrorism, allowing

---

129. *See Paris Victim's Father Sues Twitter, Facebook, Google Over ISIS*, CBS NEWS (June 15, 2016, 9:50 PM), http://www.cbsnews.com/news/paris-attacks-victim-sues-twitter-facebook-google-youtube-isis-nohemi-gonzalez/.

130. *Id.*; *see also* Jacob Bogage, *Family of ISIS Paris Attack Victim Sues Google, Facebook and Twitter*, WASH. POST (June 16, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/06/16/family-of-isis-paris-attack-victim-sues-google-facebook-and-twitter/?utm_term=.7f383919fb8e.

131. Bogage, *supra* note 130.

132. *Id.*

133. *See* Michele Gorman, *Pulse Victims' Families Sue Google, Facebook and Twitter Over ISIS Propaganda*, NEWSWEEK (Dec. 20, 2016, 5:24 PM), http://www.newsweek.com/pulse-victims-families-sue-google-facebook-twitter-isis-534407.

individuals to sue companies generally, in relation to harm caused by third parties.[134] Furthermore, as recognized by a variety of courts in litigation pertaining to the CDA, the major issue that arises in such cases involving Internet content and service providers is the impossibility of full blown monitoring and blanket bans without some form of infringement on free speech and the rights of citizens to freely post on the Internet.[135] The court in *Fields* summarized the issue nicely when it stated that, should the plaintiffs' argument succeed, "such a policy would require companies like Twitter to institute (1) expensive and likely imperfect content-specific controls or (2) broad content neutral restrictions that suppress content across the board."[136] Considering the expenses associated with such a severe monitoring program, coupled with the onslaught of litigation that these companies would face in light of the proverbial opening of the floodgates, it would not be surprising if companies shut their doors completely in the face of such exorbitant budget changes.[137] This, unlike what many of the plaintiffs are arguing, would be in direct contravention to the CDA's purpose.[138]

While it is true that a general overhaul of the CDA's liability immunity would potentially cause devastating effects to the online market, is it really good public policy to completely deny plaintiffs any sort of recourse against website providers for defamatory or illegal content posted online? To better understand plaintiffs' options under today's current CDA scheme, let us take a hypothetical character, Joe, a small-town resident who is running for a local political position in his area. Joe hears, from a friend, that a local, anonymous blog and gossip site has been spreading hurtful and defamatory rumors about him, claiming he is a drug abuser and a gambling addict, in an attempt to deter locals from voting for him. The site is anonymous, so while Joe could potentially track down the individual posters via an IP address search to discern their identity for a lawsuit, it would make more sense that Joe would want to sue the gossip site in an attempt to remove the information and gain recompense for the harm to his reputation. However, under the CDA, the gossip site is immune as a mere publisher of the third party content, unless in the course of its operations it requires defamatory or illegal posting, a unique situation that has not been brought up in any

134. Alger, *supra* note 26, at 31.

135. Fields v. Twitter, Inc., No. 16-CV-00213-WHO, 2016 WL 6822065, at *11 (N.D. Cal. Nov. 18, 2016).

136. *Id.*

137. *Id.*

138. *Id.*

scenario outside of the Ninth Circuit *Roommates.com* decision.[139] This leaves the common plaintiff out of most options, forcing him to either pursue a separate lawsuit against the individual posters, something he may not have the time or resources to do, or, if the posters are anonymous and cannot be found, this leaves him with no recourse at all. This logic applies to the antiterrorism CDA litigations as well, leaving the families of terrorism victim's helpless under the statute since most terrorist attacks are conducted abroad, the attackers are unknown, or the attackers are killed during the attack. So, what potential changes can the legislature make to the CDA to ensure that both individual citizens, as well as large-scale, online companies, are protected under the law?

While it could potentially be difficult in its application, there are two possible routes that courts, or Congress, could take to alleviate the discriminatory effect that the CDA has on the average plaintiff.[140] First, some scholars and companies have suggested that a report and remove system, coupled with an amendment to the CDA to include such scenarios in its text, might be the best answer for both individuals and companies.[141] This type of amendment would push liability onto ICSs when they are on notice of defamatory or illegal content on their site and refuse to remove it.[142] It is also important to note that in light of the rising number of terrorism related webpages and complaints that companies, like Facebook and Twitter, have been receiving, these sites have openly stated that they are employing global teams, language experts, and counterterrorism experts to review terrorism linked content, or potentially dangerous content, at all times.[143] While it could be potentially difficult for major websites to monitor posts that they receive notice of around the clock, it seems that these sites are already willing to do this, at least in connection to antiterrorism measures, and such an amendment to the CDA would further this goal.[144] Another amendment to the CDA that could lead to vast improvements in online defamation

---

139. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1175 (9th Cir. 2008).

140. *See* Burke, *supra* note 6, at 257-58; *see also* Spiccia, *supra* note 6, at 408.

141. *See* Burke, *supra* note 6, at 257-58; *see also* Spiccia, *supra* note 6, at 408.

142. Burke *supra* note 6, at 257-58.

143. *See* Alejandro Alba, *Facebook Responds to Change.org Petition Criticizing Its Anti-Terrorism Policies Following Terrorist Attacks*, N.Y. DAILY NEWS (Dec. 9, 2015, 2:02 PM), http://www.nydailynews.com/news/world/facebook-responds-criticism-anti-terrorismpolicy-article-1.2460276.

144. *See* Press Release, Facebook, Global Internet Forum to Counter Terrorism To Hold First Meeting in San Francisco (July 31, 2017), https://newsroom.fb.com/news/2017/07/global-internet-forum-to-counter-terrorism-to-hold-first-meeting-in-san-francisco/.

suits is an overhaul of the definition of an ICP.[145] Some scholars, like Michael Burke, have argued that this "would enable courts to distinguish between websites that do nothing to encourage the illegal content . . . from websites such as Roommates . . . that encourage and are aware of the illegal content being generated on the websites they operate."[146] This expanded definition could also include the aforementioned report and remove the tactic that websites, like Facebook, are starting to implement.[147] Once the ICS is notified of a defamatory or terrorist related post, it is their duty to remove the content, otherwise they run the risk of liability under both of these proposed changes.[148]

A second method of improving CDA litigation is to adopt the Ninth Circuit interpretation of the CDA that denies such expansive protection for ISPs under § 230.[149] This would mean that courts could apply the *Roommates.com* solution of determining whether the website in question has made a material contribution or has encouraged or required the posting of illegal information.[150] This could apply to sites that encourage discrimination (such as the *Roommates.com* case), sites that encourage defamation (like anonymous gossip sites), or could include websites, like Facebook, if they encourage some sort of false or illegal content to remain unchecked.[151] This would push liability beyond anonymous third parties and allow recourse against the computer services as well.[152] This could also be applied to terrorism lawsuits, allowing the families of terrorism victims to bring allegations against websites if they had an actual role in perpetrating or encouraging the illegal content posted on the site under the CDA and §§ 2339A and 2339B, both of which address material support and contributions to the illicit content.[153] Finally, this would create beneficial changes to the Internet by encouraging the shutting down or removal of harmful, rumor-based websites while encouraging "websites that serve other purposes [to] closely monitor their sites to ensure they do not do anything to encourage defamatory content."[154]

---

145. Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1175 (9th Cir. 2008); Burke, *supra* note 6, at 257-58.

146. Burke, *supra* note 6, at 257-58.

147. *Id.*

148. *Id.*

149. *Id.* at 256-57.

150. *Id.*; *see Fair Hous.*, 521 F.3d at 1175.

151. Burke, *supra* note 6, at 257-58.

152. *Id.*

153. *See* 18 U.S.C. § 2339A (2009); 18 U.S.C. § 2339B (2015); 47 U.S.C. § 230 (1998).

154. Burke, *supra* note 6, at 257.

It helps to put these possible new applications and amendments into perspective, so let us revisit the hypothetical presented earlier involving Joe, the local elections, and the gossip website. Under these new legal interpretations of the CDA or a statutory amendment, Joe could now sue the gossip site for defamation if he puts them on notice that the content is defamatory and harmful to his reputation.[155] The site could do a number of things in return. As suggested in Patricia Spiccia's article, *The Best Thing in Life Are Not Free: Why Immunity Under Section 230 of the Communications Decency Act Should Be Earned and Not Freely Given,* the site could respond to Joe, acknowledging receipt of his complaint, and then implement measures to remove the content and potentially block the user.[156] If the website fails to do so, Joe could then sue them for liability arguing that they were on notice of the defamatory content and failed to act in violation of the statute.[157] The second route that Joe could argue, if the court began implementing the Ninth Circuit's material contribution interpretation from the *Roommates.com* decision, is that the gossip site, by default, knowingly encourages the posting of defamatory information and is liable for materially contributing to the content.[158]

Joe could also argue his case via other Ninth Circuit CDA interpretations, possibly invoking the theory of promissory estoppel, like in *Barnes v. Yahoo!*, or a duty to warn, like the *Internet Brands* case.[159] However, these are fairly limited in their scope and application, and Joe would have to produce a pretty specific set of facts to invoke these two interpretations of the CDA. For example, Joe could probably bring up the theory of promissory estoppel promulgated in *Barnes* if he relied on the gossip site's assurances that they would remove the defamatory content, the content was never removed, and Joe suffered some sort of harm from the posts remaining up, which, in our hypothetical, would probably his loss of the local election.[160] Duty to warn, as seen in *Internet Brands*, would come into play if Joe suffered some sort of palpable harm or was the victim of criminal or tortious conduct after being induced by a false advertisement or posting on the website.[161] This goes to show that

---

155. *See* Spiccia, *supra* note 6, at 413-16.

156. *Id.*

157. *Id.*

158. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1175 (9th Cir. 2008); Burke, *supra* note 6, at 257-58.

159. *See* Jane Doe No. 14 v. Internet Brands, Inc., 824 F.3d 848, 848 (9th Cir. 2016); Barnes v. Yahoo!, Inc., 570 F.3d 1098, 1109 (9th Cir. 2009).

160. *See Barnes*, 570 F.3d at 1109.

161. *See Internet Brands*, 824 F.3d at 848.

while there are some more modern takes on the CDA, they are still incredibly difficult in practice.

Would these new methods of interpretation work in connection to the plaintiffs in *Fields* and other suits involving international terrorism? While it is difficult to say whether *Fields* would perfectly fit into the above scenario, these types of lawsuits would most certainly benefit from a change in legislation or new case precedent. The widows in *Fields* could connect the material support statute §§ 2993A and 2993B to the Ninth Circuit's interpretation of websites materially contributing to the posting of illegal content.[162] It would also be far easier for victims of terror and their families to sue websites, like Facebook and Twitter, under an amended CDA and a notice and report system.[163] In that instance, if Facebook was made aware of terrorist content posted by organizations, such as ISIS, either domestically or abroad, Facebook failed to remove the page, and the page or its contents were linked more directly to a specific attack or to terrorist recruitment efforts, Facebook would be liable and this would facilitate recovery for the plaintiffs.[164] It will be interesting to see whether any of these new litigations filed pertaining to terrorism encourage the U.S. courts to adopt the Ninth Circuit's perspective from cases, such as *Roommates.com*, or whether Congress is encouraged to amend § 230 of the CDA to adapt to the ever expanding prowess of the Internet. Furthermore, this issue may be one that needs to be addressed globally, as other countries begin to analyze questions of liability involving companies with such a strong global presence.

IV. THE RISE OF ONLINE ANTITERRORISM LITIGATION IN EUROPE

Lawsuits involving online defamation via terrorist propaganda pages have spread across the Atlantic into Europe, bringing up questions of individual privacy laws in conjunction with free speech. A German court in a high profile case filed by a Syrian refugee against Facebook, recently held that Facebook was immune from liability for defamatory posts made about the refugee because it had not edited the content in any way and it was not actually dispensing the information.[165] The case was filed earlier this year by Anas Modamani, a Syrian refugee living in Berlin, who posed for a selfie with German Chancellor Angela Merkel

---

162. *See Fair Hous.*, 521 F.3d at 1175 (9th Cir. 2008).

163. Burke, *supra* note 6, at 257-58.

164. *Id.*

165. *See* Melissa Eddy, *Selfie with Merkel by Refugee Became a Legal Case, but Facebook Won in German Court*, N.Y. TIMES (Mar. 7, 2017), https://www.nytimes.com/2017/03/07/business/germany-facebook-refugee-selfie-merkel.html?_r=0.

back in 2015.[166] The photo went viral throughout Germany, and Modamani became a major symbol for Merkel's views on immigration and for refugees throughout Germany.[167] However, the photo was also manipulated and used in Facebook posts falsely linking Modamani to terrorist attacks throughout Europe including the Brussels attacks, the Berlin Christmas market attack, as well as an especially disturbing attack involving a homeless man in Berlin.[168] Modamani brought suit in the court of Wurzburg in February 2017 seeking an injunction against Facebook, requiring them to remove any and all content that connected him to terrorism in any way.[169]

Modamani's argument centered around the German Constitution, which "guarantees a right to the 'free development of the individual,' which is understood to include the right to personal privacy and to determine the extent to which a person appears in public."[170] Modamani also requested that the defamatory content be removed from Facebook, which Facebook failed to do in full.[171] Facebook countered by arguing that it had no feasible way of knowing every page that used Modamani's picture in a defamatory manner, making it impossible for them to remove and block all of the content as requested.[172] The German court, taking an approach similar to courts in the United States, found that Facebook was not liable for the defamatory content pertaining to Modamani because it "had not in any way manipulated the content, which would have made it legally responsible for the distribution."[173] The judge also invoked European Union (EU) law, stating that "a host provider . . . could be held responsible for eliminating content from its site only when it was considered technically possible."[174] Because Facebook had testified that it would be impossible to remove all of the content pertaining to Modamani, even when placed on notice of the defamatory posts, Modamani's argument failed under EU law as well as local law.[175]

The Modamani selfie case highlights the important struggle between personal privacy and social media outlets that courts in the EU are facing on a more frequent basis, like the United States. The German

166. *Id.*
167. *Id.*
168. *Id.*; *see* Eddy, *supra* note 7.
169. *See* Eddy, *supra* note 7.
170. Eddy, *supra* note 165.
171. *Id.*
172. *Id.*
173. *Id.*
174. *Id.*
175. *Id.*

court, in an argument similar to those seen in the United States, found that the third party responsible for the post and its contents is liable to Modamani, but Facebook escapes under both state and EU law.[176] Furthermore, the court upheld the idea that Facebook, which has processes for removing inappropriate content and flagging dangerous posts, can still escape liability even when it is on notice that posts may be illegal or harmful in nature.[177] It is also important to note that another German court in Bremen sentenced a man to prison for six months and two weeks for insulting refugees on a Facebook page, yet Facebook itself was not involved.[178] This further supports the idea that while third parties are legally responsible for content they post online, Facebook remains free of liability, even in the most extreme cases of defamation.

Germany and other EU countries must also answer the question, what can the courts do to change the outcome of such cases and offer compensation to those whose reputation is harmed online? Similar to the United States, the answer remains unclear. Yet, advocates for individual rights in Germany and other countries in the EU argue that the Modamani case is an important step in shifting online liability as it points out which specific laws need to be adjusted to protect individuals' privacy online.[179] Germany is a country that is especially concerned with the implication of online propaganda since it may pose a risk to the country's elections coming up next September.[180] For now, it seems that the EU is sticking to a similar analysis to America, granting immunity to social media sites based on the sheer size of these companies, coupled with the potential risk for increased numbers of lawsuits should the law be amended or changed. It may be beneficial for Europe to introduce a report and remove policy, as has been suggested in the United States, or to amend EU e-commerce laws or local laws to reflect online terrorist propaganda and defamation in a clearer manner.[181]

Despite these cases springing up in various courts around the globe, seemingly identical types of claims are being analyzed in a similar fashion, and courts in various countries are having to figure out how to address issues of individual privacy in the online era. Tech giants, like Facebook, whose presence has expanded beyond the United States to assume a global role, may actually produce the most effective and

176. *Id.*
177. *Id.*
178. *Id.*
179. *Id.*
180. Eddy, *supra* note 7.
181. *See* Burke, *supra* note 6, at 257-58; *see also* Spiccia, *supra* note 6, at 408.

positive change for Internet-related lawsuits should the onus be on them to take the first steps at preventing online defamation and terrorism. Sites have already begun to institute antiterrorism and antidefamation departments whose responsibility it is to respond to posts that have been flagged as dangerous. It is quite possible that if a company, like Facebook, took the reins and began implementing global, site-wide policies, such as a notice and report system that applied worldwide, this could prompt courts, particularly in technology heavy areas, like the United States, Europe, and Asia, to adapt their laws to protect consumers more effectively. If Facebook's actions prompted responses from the U.S. Supreme Court and high EU courts, like the European Court of Justice, this could have immensely beneficial effects for future online consumers. While courts worldwide are presently remaining on the side of companies in defamation and terrorist litigation, these problems will endure as the Internet continues to take on a more important role in the daily lives of U.S. and foreign consumers.

In conclusion, the answer to how we can make the Internet a more welcoming place for plaintiffs remains unclear. However, it is encouraging to see courts beginning to analyze these issues of terrorism, defamation, and damaged reputation in a more consumer-oriented light. Some courts, like the U.S. Ninth Circuit, are beginning to devise crafty ways around publisher immunity, and lawyers are taking creative arguments, like promissory estoppel, duty to warn, material support to terrorist organizations, and placing the website on notice, to protect individuals harmed locally and abroad. As the Internet continues to take on a stronger presence worldwide, it is inevitable that the current legislation will need to be revisited and adapt to the modern Internet user.