# TO CATCH A CATFISH:

# A STATUTORY SOLUTION FOR VICTIMS OF ONLINE IMPERSONATION

COLLEEN M. KOCH*

*Though popular MTV reality show Catfish makes online impersonation seem like a lighthearted and incredible harm, it is actually an undesirable cyber behavior that carries potentially serious consequences. Despite the seriousness of the problem, social networking sites have few incentives to stop the problem, largely due to the broad immunity they are granted by Section 230 of the Communications Decency Act, which holds them entirely immune for the content posted by users of their sites. Moreover, few state statutes currently exist to address the problem, and those that do are largely ineffective. While civil liability could be a solution to the problem, as the law currently stands, most civil remedies are too costly to pursue given the relatively low damages available to plaintiffs. Thus, amending Section 230 to hold social networking sites liable for harmful online impersonation about which they have actual knowledge, in an amendment similar to that of the Digital Millennium Copyright Act that holds websites liable for copyright-infringing material they knew or should have known about, would allow and encourage both (1) stronger enforcement of existing terms of service agreements on social media sites, and (2) civil litigation to protect an individual's right to Internet safety and freedom when social media sites fail to do so.*

* J.D. Candidate, 2017, University of Colorado Law School; Managing Editor, *University of Colorado Law Review*. Thank you to all the members of the *Colorado Law Review* who gave me their invaluable advice and edits on this Comment, in particular Jessica Pingleton, Anna Adams, and Stephanie Drumm. Special thanks to my fellow executive board members, Casey Klekas and Hope Griffin, for always being a wonderfully supportive team. Most of all, thank you to my husband Andy, for all you do for our family, and for coming up with an interesting Comment topic during a late-night reality TV binge. Everything I do is possible because of you.

INTRODUCTION ..... 234
I. BACKGROUND ..... 239
A. *What is Online Impersonation?* ..... 239
B. *How Does Online Impersonation Harm Victims?* ..... 242
1. Social Harms ..... 242
2. Cyberbullying ..... 245
3. Other Serious Dangers ..... 246
II. A LACK OF INCENTIVES ..... 248
A. *Current Social Media Network Policies to Stop Online Impersonation* ..... 249
B. *Financial Incentives* ..... 251
C. *Section 230 of the Communications Decency Act* ..... 253
III. THE TROUBLE WITH STATE ENFORCEMENT ..... 256
A. *Current State Efforts* ..... 257
B. *Why Criminal Statues are Ineffective* ..... 258
C. *The Benefits of Civil Enforcement* ..... 261
D. *Potential Civil Causes of Action* ..... 262
1. Misappropriation of Likeness ..... 263
2. Defamation ..... 263
3. Intentional Infliction of Emotional Distress ..... 264
4. Fraudulent Misrepresentation ..... 265
E. *What Problems Might Arise With Private Litigation?* ..... 266
IV. A NATIONAL ISSUE ..... 267
A. *What Existing Federal Laws Address Cybercrimes?* ..... 268
B. *A Need for Change Within Section 230* ..... 270
C. *The Digital Millennium Copyright Act* ..... 273
D. *A Proposed Amendment* ..... 275
E. *Potential Problems with an Amendment* ..... 277
CONCLUSION ..... 279

## INTRODUCTION

On May 10, 2012, Chris Andersen's life changed forever.[1] While driving to a team practice at the Pepsi Center, the then-member of the Denver Nuggets, more commonly known as "Birdman," noticed several police cars following him.[2] When he

1. Flinder Boyd, *The Birdman's Vengeful Ghost*, NEWSWEEK (May 28, 2014, 5:58 AM), http://www.newsweek.com/2014/06/06/birdmans-vengeful-ghost-252517.html [https://perma.cc/NU3S-GZN4].

2. *Id.*

stopped, police officers informed him that officers from the Douglas County Sheriff's Office, including members of the Internet Crimes Against Children Unit (ICAC), were going to his home to execute a search warrant.[3] After being sent home early from practice, Andersen drove past the media trucks lined up outside his house.[4] He pushed through the crowd gathered on his driveway, and walked in to see that the sheriffs had confiscated his Xbox and his computer, and had broken into his safe.[5] Although initially the police would not tell him why he was being investigated, Andersen saw on television that ICAC, "which deals with everything from possession of child pornography to child rapists," was involved.[6] Their involvement led regional news channels and social media outlets like Facebook and Twitter to depict Andersen as a child molester.[7]

Earlier that same year, Andersen had been the victim of an extortion plot, stemming from a brief relationship he had with aspiring model Paris Roxanne.[8] Initially, when Andersen and Roxanne met on Facebook, she claimed to be twenty-one years old.[9] After communicating regularly via Facebook, the pair spent a few days together in Denver, eventually engaging in consensual sex.[10] The relationship fizzled out, and communication ended between the two.[11] However, Andersen later received threatening messages from someone claiming to be Roxanne's mother, telling him that Roxanne was actually only seventeen years old and demanding money in exchange for keeping the story quiet.[12] Though Andersen had not broken any laws (the legal age of sexual consent in Colorado is seventeen)[13], he agreed to send a small amount of money to an undisclosed location in order to avoid any negative publicity.[14]

At the same time, Roxanne, who knew nothing about the extortion involving Andersen, received threatening messages

3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*
7. *Id.*
8. *Id.*
9. *Id.*
10. *Id.*
11. *Id.*
12. *Id.*
13. COLO. REV. STAT. § 18-3-402(1)(d) (2016).
14. Boyd, *supra* note 1.

as well.[15] Someone purporting to be Andersen threatened her with harm and asked her to perform degrading sex acts.[16] Roxanne notified authorities, and the Douglas County Sheriff's Office obtained a warrant to search Andersen's home.[17] With the media sitting outside his house awaiting any news, Andersen was forced to stay home for days, missing the deciding game in the Nuggets' playoff series against the Los Angeles Lakers.[18]

During the ICAC's investigation, Andersen was released from the Nuggets.[19] However, the investigation—which initially appeared like an open-and-shut child pornography case due to the nude photographs of seventeen-year-old Roxanne found on Andersen's hard drive—took a surprising twist when investigators uncovered that Roxanne and Andersen's electronic interactions had not been intimate conversations between the two of them, but rather triangulated through a third person.[20] Shelly Lynne Chartier, a small-town recluse and prolific online impersonator,[21] had created fake Facebook profiles for both Andersen and Roxanne, manipulating the interactions so that each person thought he or she was talking to the true person, not a stranger hidden behind a computer screen.[22] And although Andersen's name was eventually cleared, the damage was already done; with an open investigation underway, new NBA teams were hesitant to sign a contract with a potential child-sex criminal.[23] It took

15. *Id.*
16. *Id.*
17. *Id.*
18. *Id.*
19. *Id.* Andersen also had a difficult season, but the pending police investigation against him was a factor in the team's decision to end his contract. *See* Benjamin Hochman, *Nuggets Cut Chris "Birdman" Andersen and Sign Anthony Randolph*, DENVER POST (July 17, 2012, 8:24 PM), http://www.denverpost.com/ci_21097577/nuggets-cut-chris-birdman-andersen [https://perma.cc/GA87-CGH4].
20. Boyd, *supra* note 1.
21. Chartier was involved in multiple online impersonation schemes prior to her conviction and incarceration for these online crimes. Her victims, in addition to Andersen, included several professional athletes, Playboy models, and reality-television personality Brody Jenner. Mike McIntyre, *Meet Shelly Chartier: An Exclusive Jailhouse Interview with the Reclusive, Celebrity-Obsessed Con Artist*, WINNIPEG FREE PRESS (Nov. 5, 2015, 6:00 PM), http://www.winnipegfreepress.com/local/Meet-Shelly-Chartier-341117762.html [https://perma.cc/LPU4-2D3L].
22. Boyd, *supra* note 1.
23. *Id.*

until the middle of the NBA season for Andersen to get a probationary contract with the Miami Heat and over a year from the initial investigation for his name to be officially cleared.[24] While Andersen has gone on to have a successful career with the Heat, he has transformed from a charismatic, memorable player to a recluse—in part due to the online impersonation scheme of which he was a victim.[25]

Although Andersen's story is an extreme version, online impersonation is a surprisingly common occurrence. For example, although Facebook estimated in its 2015 filing that less than five percent of its accounts were duplicates,[26] that seemingly small percentage takes on new meaning when considered in conjunction with the fact that Facebook is the world's most popular social network, with over one billion Monthly Active Users,[27] meaning that in 2015 alone, there were over fifty million duplicate accounts.[28] Online impersonation, or "catfishing," is when a "catfish" "sets up a false person profile on a social networking site for fraudulent or deceptive purposes."[29] The term was coined by the documentary *Catfish*,[30] which followed Nev Schulman, a filmmaker involved in an online relationship, as he discovered that the beautiful woman in the photographs sent to him was not the person he had been talking to at all, but rather a middle-aged homemaker who gave up her career to care for her intellectually disabled son.[31] The movie spawned a reality

24. *Id.*

25. *Id.* Andersen now avoids children's homes and hospitals and sold his house to move to a more secluded area. *Id.*

26. A duplicate account is defined as "an account that a user maintains in addition to his or her principal account." Facebook, Annual Report 2015, at 8 (Form 10-K) (Jan. 25, 2016), https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/2015-Annual-Report.pdf [https://perma.cc/5MZ7-FZ9U]. A duplicate account does not necessarily mean the account is an impersonation of another, although accounts impersonating existing users would fall under this definition.

27. *Number of Monthly Active Facebook Users Worldwide as of 3rd Quarter 2015*, STATISTA, http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (last visited Nov. 13, 2015) [https://perma.cc/HUR5-MKPT].

28. Assuming one billion accounts of which five percent were duplicates.

29. *Catfish*, MERRIAM-WEBSTER, www.merriam-webster.com/dictionary/catfish (last visited Sept. 26, 2015) [https://perma.cc/8MG2-FL9Q].

30. *Catfish*, IMDB, http://www.imdb.com/title/tt1584016/?ref_=fn_al_tt_1 (last visited Oct. 2, 2015) [https://perma.cc/2PFR-8MX8].

31. *Synopsis for Catfish*, IMDB, http://www.imdb.com/title/tt1584016/synopsis?ref_=ttpl_pl_syn (last visited Oct. 15, 2015) [https://perma.cc/SJ6X-

television show on MTV bearing the same name. The show, still currently on-air, is meant to help people discover the true identity behind the online profile with which they have been corresponding.[32]

Despite the dangers of online impersonation remaining unchecked, victims are left largely without an adequate remedy. Section 230 of the Communications Decency Act (Section 230) grants broad immunity to website operators[33] for the harmful publications of others.[34] Moreover, only a few states criminalize the behavior,[35] and what few criminal statutes exist are largely ineffective in prosecuting online crimes and protecting victims due to their failure to appropriately account for the breadth of undesirable cyber behavior and the rapidly changing online landscape.[36] But if the barrier to successful suit created by Section 230 were removed by federal statute, website operators would have a greater incentive to monitor and stop harmful digital behavior, and victims of online impersonation could have a successful remedy in tort.

Thus, in light of the damaging consequences of online impersonation, there should be a path to recovery for victims. Using the Digital Millennium Copyright Act as a guide, this Comment proposes an amendment to Section 230. If passed, it

SZR9]. The unusual title for the documentary came from the film's online impersonator's husband. In describing his wife, he said, "They used to tank cod from Alaska all the way to China. They'd keep them in vats in the ship. By the time the codfish reached China, the flesh was mush and tasteless. So this guy came up with the idea that if you put these cods in these big vats, put some catfish in with them and the catfish will keep the cod agile. And there are those people who are catfish in life. And they keep you on your toes. They keep you guessing, they keep you thinking, they keep you fresh. And I thank god for the catfish because we would be droll, boring, and dull if we didn't have somebody nipping at our fin." Aisha Harris, *Who Coined the Term "Catfish"?*, SLATE: BROWBEAT: SLATE'S CULTURE BLOG (Jan. 18, 2013, 4:00 PM), http://www.slate.com/blogs/browbeat/2013/01/18/catfish_meaning_and_definition_term_for_online_hoaxes_has_a_surprisingly.html [https://perma.cc/U99R-DZJ3].

32. *About Catfish: The TV Show*, MTV.COM, www.mtv.com/shows/catfish (last visited Sept. 26, 2015) [https://perma.cc/4NFQ-TEUF].

33. The Act utilizes the term "provider of an interactive computer service" to describe website operators and hosts such as Facebook. *See* 47 U.S.C. § 230(c)(1) (2012). However, for the purposes of clarity and brevity, this Comment will use the term "website operator."

34. *See infra* Section II.C.

35. *See infra* Section III.A.

36. *See, e.g.*, Larry Downs, *The Fallacy of "E-Personation" Laws*, TECHNOLOGY LIBERATION FRONT (June 11, 2010), http://techliberation.com/2010/06/11/the-fallacy-of-e-personation-laws/ [https://perma.cc/V8BT-E2CB].

would narrow the immunity granted to website operators in cases where the operator had knowledge of harmful content and did not remove it. This proposed amendment would serve two purposes: (1) incentivize website operators, such as operators of social media sites, to remove harmful content when it is reported and (2) allow recourse for victims of online impersonation should social media networks fail to protect them.

Part I provides background information on online impersonation in general, including the dangers it poses. Part II examines the lack of incentives for social media networks to address the problem themselves, including the current policies in place that attempt to stop online impersonation, the lack of financial incentives to further stop the problem, and the immunities granted by Section 230. Part III discusses the current state enforcement options and the problems they pose, as well as potential civil causes of action. Finally, Part IV explains why online impersonation is best addressed on a national level by examining the need for change within the current statutory scheme and proposing an amendment to Section 230.

## I. BACKGROUND

While MTV's *Catfish* may occasionally make light of online impersonation, it is actually part of a wider kaleidoscope of undesirable and potentially harmful online conduct that can lead to serious consequences for victims. This Section examines what online impersonation is and explores the harms caused by online impersonation, including the dangers of cyberbullying and cyberstalking.

### *A. What is Online Impersonation?*

Online impersonation is part of a larger, ill-defined area of the law governing undesirable online behavior. Within this broader category of undesirable cyber behavior is also (1) cyberbullying, (2) cyberharassment, and (3) cyberstalking. Cyberbullying is generally defined as "the willful and repeated use of cell phones, computers, and other electronic

communication devices to harass and threaten others."[37] While cyberbullying is typically confined to discussions within the school context,[38] cyberharassment is a more general term encompassing threatening or harassing online or electronic communications "dedicated solely to tormenting an individual."[39] In addressing the issue of cyberharassment, some states have added provisions to their existing harassment laws, while others have created stand-alone cyberharassment statutes.[40] The most sinister of cybercrimes, cyberstalking, is the use of electronic or online communications to stalk another and typically encompasses threatening or malicious behavior.[41]

The fake profiles generated through online impersonation are harmful not only to the person who interacts with the profile, as in the cases of cyberharassment or cyberbullying, but also to the people whose pictures are co-opted. Aimee Gonzales, the model whose photos were used to create the fake profile depicted in the movie *Catfish*, explained, "[I]t's almost

37. *Cyberbullying*, NAT'L CONF. OF STATE LEGS., http://www.ncsl.org/research/education/cyberbullying.aspx (last visited Oct. 2, 2015) [https://perma.cc/6K95-RMXX]; *see infra* Section I.B.2.

38. *See* Kori Clanton, Comment, *We Are Not Who We Pretend to Be: ODR Alternatives to Online Impersonation Statutes*, 16 CARDOZO J. CONFLICT RESOL. 323, 330 (2014) ("It helps to think of cyberbullying as an umbrella term that encompasses a broad range of impermissible online conduct often discussed in the context of education.").

39. *State Cyberstalking, Cyberharassment and Cyberbullying Laws*, NAT'L CONF. OF STATE LEGS. (Aug. 3, 2011), http://lexisnexis-law-school.blogspot.com/2011/08/state-cyberstalking-cyberharassment-and.html [https://perma.cc/X7UZ-JY3V].

40. *Id.* For example, Alabama amended its criminal harassment statute in 1997 to make the crime of "harassing communications" independent of harassment. 1997 Ala. Laws 97-552. Section 13A-11-8(b)(1)(a) now criminalizes communicating with a person via electronic communication "in a manner likely to harass or cause harm." ALA. CODE § 13A-11-8(b)(1)(a) (LexisNexis 2016). Colorado is more specific; Section 18-9-111(1)(e) explicitly mentions harassment via "data network, text message, instant message, computer, computer network, computer system, or other interactive computer medium" within its harassment statute. COLO. REV. STAT. § 18-9-111(1)(e) (2015). By contrast, Arkansas added Section 5-41-108 to its criminal code in 1997, criminalizing unlawful computerized communications, including sending a message threatening another person or using obscene language with the "purpose to frighten, intimidate, threaten, abuse, or harass." 1997 Ark. Acts 1153; ARK. CODE ANN. § 5-41-108(a)(1)–(2) (2015).

41. *State Cyberstalking, Cyberharassment and Cyberbullying Laws*, *supra* note 39. Also within the realm of cybercrimes, but outside the scope of this Comment, is identity theft, which typically has a financial motive. *See Identity Theft*, U.S. DEP'T OF JUSTICE, http://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud (last visited Nov. 12, 2015) [https://perma.cc/465M-4ZU4].

worse than stealing someone's name. She actually stole my face. There's nothing more than your face that makes you who you are."[42] Beyond just using Gonzales's photos, the impersonator extensively followed Gonzales online, even using her quotations as captions for the stolen photographs.[43] In another bizarre online impersonation story, Jennifer Lopez found herself the subject of a lawsuit and police report filed by a complete stranger, who claimed Lopez had mailed him a letter demanding he reply with nude photographs.[44]

Despite the sometimes incredible-sounding premise of online impersonation schemes, cultural changes have allowed impersonators to have more success in duping their intended targets or impersonating others. In the modern era, the understanding of the word "friend" has shifted, with many online users creating "friendships" with other users with whom they have not had traditional interactions.[45] This broader definition of "friend" has led to the "breakdown of traditional social barriers that kept strangers apart. This reshaping of human interaction has progressed to the point where individuals have 'dating' relationships completely online."[46]

Furthermore, once an individual is in an online relationship, social media is able to imitate face-to-face interactions in a way that other forms of remote interaction cannot.[47] Impersonators are able to craft idealized personas, commanding the victim's trust and confidence, especially because written messages can be read and re-read, causing them to have a stronger impact and feel more "real."[48] This "more real" interaction causes users to believe that the person on the other end of the relationship is who he or she purports

42. Gina Piccalo, *Catfish's Photo Fraud Victim*, DAILY BEAST (Oct. 4, 2010, 6:38 PM), http://www.thedailybeast.com/articles/2010/10/04/catfish-aimee-gonzales-speaks-out.html [https://perma.cc/C2SW-C2RT].

43. *Id.*

44. Chiderah Monde, *Jennifer Lopez Sued by Los Angeles Man for Bizarre 'Nude Pictures' Scam: Report*, N.Y. DAILY NEWS (Jan. 12, 2014, 2:51 PM), http://www.nydailynews.com/entertainment/gossip/jennifer-lopez-sued-man-nude-pictures-scam-report-article-1.1577057 [https://perma.cc/7NZK-FQ9Y].

45. Thaddeus Hoffmeister, *The Challenges of Preventing and Prosecuting Social Media Crimes*, 35 PACE L. REV. 115, 130–31 (2014).

46. *Id.*

47. *Id.* at 130.

48. Doug Shadel & David Dudley, *'Are You Real?'—Inside an Online Dating Scam*, AARP THE MAGAZINE (June/July 2015), http://www.aarp.org/money/scams-fraud/info-2015/online-dating-scam.html [https://perma.cc/Y7FP-SQLX].

to be,[49] especially when emotions and confirmation bias take over,[50] allowing an impersonator to continue his or her scheme with greater confidence.

### *B. How Does Online Impersonation Harm Victims?*

Online impersonation poses potentially serious risks for victims, both those who are impersonated and those who fall for the scam. These harms can be felt on either side of the scheme, depending upon how the impersonator behaves once the fake profile is created. "Given the widespread and growing adoption of social media, an individual's online persona is often the first impression that friends, potential romantic partners, and employers have of them."[51] False online impersonation can cause social harms, including problems with employment, relationships, and finances; it can also be part of more dangerous situations, such as cyberbullying and other cybercrimes.

#### 1. Social Harms

Online impersonation can lead to a victim's social reputation being damaged, which can in turn affect employment and personal relationships. Currently, there are no regulations regarding an employer's use of social media as a tool for screening applicants.[52] In a 2014 survey, CareerBuilder.com found that 43 percent of employers research applicants on social media.[53] Additionally, 51 percent of those employers who researched job candidates online found content that made them decide not to hire the applicant.[54] In a 2013 study, 77 percent of employers reported using social media to recruit candidates for specific jobs.[55] When asked what sorts of

49. Hoffmeister, *supra* note 45, at 130.

50. Shadel & Dudley, *supra* note 48.

51. Clanton, *supra* note 38, at 326.

52. Francois Quintin Cilliers, *The Role and Effect of Social Media in the Workplace*, 40 N. KY. L. REV. 567, 568 (2013).

53. *Number of Employers Passing on Applicants Due to Social Media Posts Continues to Rise, According to New CareerBuilder Survey*, CAREERBUILDER (June 26, 2014), http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=6%2F26%2F2014&id=pr829&ed=12%2F31%2F2014 [https://perma.cc/E636-ZAPY].

54. *Id.*

55. Jonathan A. Segal, *Social Media Use in Hiring: Assessing the Risks*,

reputational information influenced decisions to reject an applicant, employers identified things like "inappropriate comments and text written by the candidate," "unsuitable photos, videos, and information," "poor communication skills displayed online," and "discover[ing] that information the candidate shared was false."[56] An online impersonator could create content that addresses all of these with little to no actual knowledge about his or her victim. If an online impersonator were to post a page, claiming to be an individual who is being considered for a new job, and the page included information a potential employer found objectionable, it could cost the real individual a job opportunity.

Similarly, online impersonation can have disastrous consequences for online daters. A 2015 study found that 20 percent of adults between the ages of twenty-five and thirty-four have used an online dating site, as have a significant number of older daters.[57] "[T]he appeal of an online relationship is that two people can present themselves to each other in an idealistic way," says Larry Bloom, a professor of psychology of human sexuality at Colorado State University.[58] Online dating allows users to carefully plan their words and hide their imperfections.[59] The temptation to present oneself in an idealized manner, though, can lead some to take it too far.

Moreover, online dating has a very sinister side. In 2006, fifty-two percent of online daters said they did not find online dating dangerous.[60] This false sense of security is heightened when users pay for the dating service.[61] In 2012, after a woman was assaulted by a man she met on Match.com, three major online dating services—Match.com, eHarmony, and

SOCIETY FOR HUMAN RESOURCE MANAGEMENT, http://www.shrm.org/publications/hrmagazine/editorialcontent/2014/0914/pages/0914-social-media-hiring.aspx (last visited Nov. 14, 2015) [https://perma.cc/3LNJ-U7DF].

56. DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 9 (2014).

57. Aaron Smith & Monica Anderson, *5 Facts about Online Dating*, PEW RESEARCH CENTER (Apr. 20, 2015), http://www.pewresearch.org/fact-tank/2015/04/20/5-facts-about-online-dating/ [https://perma.cc/5X2Z-9QKK].

58. Taylor Pettaway, *MTV's Catfish Casting for Colorado's Online Daters*, ROCKY MOUNTAIN COLLEGIAN (May 7, 2013, 4:21 PM), http://www.collegian.com/2013/05/mtvs-catfish-casting-for-colorados-online-daters/32355/ [https://perma.cc/RA6Y-XNWK].

59. *Id.*

60. Maureen Horcher, Comment, *World Wide Web of Love, Lies, and Legislation: Why Online Dating Websites Should Screen Members*, 29 J. MARSHALL J. COMPUTER & INFO. L. 251, 252 (2011).

61. *Id.*

Spark.com—agreed to screen their users for sex offenders, identity theft, and violent crimes via a joint statement of business principles.[62] However, this statement is nonbinding and carries no enforcement provisions.[63] Even with these safeguards in place, it is still possible for would-be offenders to create a profile and attract new victims. Additionally, Internet users can begin online relationships on more general social media sites without the protections offered by subscription services.[64] For example, a San Diego woman became a stalking victim after an online impersonator used her photographs to begin an online relationship with another individual.[65] When the stalker realized the impersonator was not the woman depicted in the photographs, he discovered the victim's true identity and formulated a plan to kill her and her boyfriend.[66]

Online impersonation comes with financial risks created by impersonators and other dangerous individuals as well. After creating a fake profile and gaining a victim's trust, an impersonator can dupe the victim into sending money, sometimes thousands of dollars.[67] For example, Denver attorney Jim Avery's photographs were stolen and used to create a fake online dating profile.[68] The impersonator then used the profile to scam the victim—an innocent woman—out

62. Associated Press, *Online Dating Sites Agree to Screen Sex Offenders*, N.Y. DAILY NEWS (Mar. 20, 2012, 8:32 PM), http://www.nydailynews.com/news/online-dating-sites-agree-screen-sex-offenders-article-1.1047863 [https://perma.cc/5UAA-HR3P].

63. Robert Jablon, *Three Online Dating Sites Agree to Screen for Predators*, USA TODAY (Mar. 21, 2012, 12:24 PM), http://usatoday30.usatoday.com/news/health/wellness/story/2012-03-21/Three-online-dating-sites-agree-to-screen-for-predators/53683868/1 [https://perma.cc/6JN9-2R7E].

64. One study suggested that seven percent of people who were married between 2005 and 2012 met through social media websites. Tia Ghose, *Love Connection: Facebook Gets Credit for Lasting Marriages*, LIVESCIENCE (Feb. 13, 2014, 2:10 PM), http://www.livescience.com/43369-social-media-marriages-work.html [https://perma.cc/EJ8J-Q9PB].

65. Monica Garske, *Man Accused of Stalking Woman in "Catfish" Dating Hoax*, NBC 7 SAN DIEGO (Aug. 29, 2013, 5:06 PM), http://www.nbcsandiego.com/news/local/Brian-Curtis-Hile-Insterstate-Stalking-Catfish-Online-Dating-Scam-221721421.html [https://perma.cc/9CBT-68XY].

66. *Id.*

67. *Online Dating and Romance Scams*, OFFICE OF MINN. ATTORNEY GEN. LORI SWANSON, https://www.ag.state.mn.us/Consumer/Publications/OnlineDatingRomanceScams.asp (last visited Nov. 13, 2015) [https://perma.cc/THB8-CQ9Y].

68. *Comment: Dr. Phil Show about "Catfish" Dating Scam*, AVERY LAW FIRM, http://www.coloradosuperlawyer.com/comment-dr-phil-show-about-catfish-dating-scam/ (last visited Oct. 2, 2015) [https://perma.cc/9VRH-25BT].

of over $190,000.[69] In 2013, a Federal Trade Commission report stated that there were over $105 million in losses as a result of romance scams.[70] In a romance scam, an online impersonator will create a fake profile, trick his or her victim into sending intimate photographs or videos, and then demand money to keep the pictures private.[71] Furthermore, the FBI reported that American victims lost roughly $82 million to online dating fraud in the last six months of 2014 alone.[72]

Through the creation and maintenance of false online personas, online impersonators are able to perpetrate a variety of undesirable behaviors online, including more serious cybercrimes like cyberbullying.

2. Cyberbullying

Cyberbullying presents unique concerns for Internet users and school administrators. The National Crime Prevention Council reported that forty-three percent of teenagers have been victims of cyberbullying.[73] Of these, nearly twenty percent were cyberbullied via online impersonation, being fooled by an impersonator into revealing personal information.[74] Thirteen percent of victims learned that a cyberbully was pretending to be them while harassing someone else.[75]

Perhaps the most well-known case at the intersection of online impersonation and cyberbullying is the Megan Meier case.[76] In that case, Lori Drew, the mother of one of thirteen-year-old Meier's classmates, wanted to gain insight into Meier's thoughts about her own daughter.[77] In order to gain Meier's

69. *Id.*

70. Sean Allocca, Ed., *Online-Dating Extortion Scams Exposed*, DFI NEWS (Mar. 12, 2015), http://www.forensicmag.com/articles/2015/02/online-dating-extortion-scams-exposed [https://perma.cc/WB2L-5RAN].

71. *Id.*

72. Shadel & Dudley, *supra* note 48. The online dating industry is estimated to be worth approximately $2 billion. *Id.* Additionally, the prevalence of online dating scams has given rise to Romancescams.org, an online support group and learning center. ROMANCE SCAMS, http://romancescams.org/WhoWeAre.html (last visited Aug. 20, 2016) [https://perma.cc/RN2G-25UM].

73. NAT'L CRIME PREVENTION COUNCIL, STOP CYBERBULLYING BEFORE IT STARTS, http://www.ncpc.org/resources/files/pdf/bullying/cyberbullying.pdf (last visited Nov. 15, 2015) [https://perma.cc/EU75-FVS2].

74. *Id.*

75. *Id.*

76. *See infra* INTRODUCTION.

77. Atticus N. Wegman, *Cyberbullying and California's Response*, 47 U.S.F. L.

trust, Drew created a fake MySpace page, holding herself out as a sixteen-year-old boy.[78] After an alleged online romance blossomed, though, the tone of Drew's messages changed, telling Meier that "everybody hates you" and that "[t]he world would be a better place without you."[79] Meier committed suicide as a result of these remarks.[80] While Drew was initially found guilty of three misdemeanors by a jury, the judge overturned the verdict due to concerns that the prosecution's argument—claiming that Drew's violation of the MySpace terms of service was criminally punishable under a federal computer hacking statute—would ultimately criminalize breach of contract.[81]

In a more recent case, several fifth-grade students created false social media accounts on multiple websites for the purpose of convincing another female student that one of the impersonating students was planning on committing suicide.[82] The repeated messages eventually caused the young girl so much anguish and anxiety that she too committed suicide.[83]

3. Other Serious Dangers

The relative ease with which a perpetrator can create a fake profile can lead to the commission of much more serious cybercrimes as well, with far-reaching consequences.[84] Online impersonation can escalate into more serious crimes, like

REV. 737, 745 (2012).

78. *Id.*

79. *Id.* at 745–46.

80. *Id.* at 746.

81. Kim Zetter, *Judge Acquits Lori Drew in Cyberbullying Case, Overrules Jury*, WIRED (July 2, 2009, 3:04 PM), http://www.wired.com/2009/07/drew_court/ [https://perma.cc/ZFJ2-97A9].

82. Lauren Zumbach, *Suit: Social Media Prank Led to 5th-grader's Suicide*, CHICAGO TRIBUNE (June 5, 2015), http://www.chicagotribune.com/news/local/breaking/ct-suit-social-media-prank-leads-to-5th-graders-suicide-20150605-story.html [https://perma.cc/WSX4-7DPV].

83. *Id.*

84. Warren Chik, *Harassment Through the Digital Medium: A Cross-Jurisdictional Analysis on the Law on Cyberstalking*, 3 J. INT'L COM. L. & TECH. 13, 14 (2009) ("[T]he [online] medium is also important for its many implications. First, the ease of use and hence lesser impediments to aggressive behavior; second, the borderless nature of electronic communications medium and concomitant jurisdictional concerns; third, the type of evidence and means of its collection; fourth, the lack of educative and deterrent effect of current laws; and fifth, the lack of effective laws, or of any law at all, to deal with the problem in some countries and in the international fora.").

cyberharassment and cyberstalking, which in turn can escalate into assault, rape, and real-world stalking.[85] While there are varying definitions, in general, cyberharassment is distinguishable from cyberstalking in that it usually is persistent enough to be considered a "course of conduct"; cyberstalking requires a reasonable fear for one's safety.[86] The U.S. Department of Justice has suggested that 850,000 adults, most of whom are women, have been victims of cyberstalking each year.[87] Another study found that forty percent of Internet users have experienced cyberharassment.[88] The unique characteristics of the Internet make these cybercrimes possible, and often more damaging than traditional harassment or stalking.[89]

Cyberstalking and cyberharassment can have long-lasting financial impact on victims. Cyberstalking can cost victims more than $1,200.[90] A recent study showed that victims of online stalking take more defensive measures, "pay higher out-of-pocket costs, and experience greater fear over time than individuals who are stalked offline," causing the financial burden imposed by these crimes to grow.[91] Further costs can come from legal fees, professional problems, child-care costs, and moving expenses.[92] Moreover, as a result of the emotional harm and distress that result from cybercrimes, victims often struggle with anxiety, leading them to seek out professional support—if they can afford it.[93]

Even more alarmingly, crimes that begin as online impersonation can escalate to real-world assaults—or worse.

85. CITRON, *supra* note 56, at 5.

86. *Id.* at 3.

87. Marlisse Silver Sweeney, *What the Law Can (and Can't) Do About Online Harassment*, ATLANTIC (Nov. 12, 2014), http://www.theatlantic.com/technology/archive/2014/11/what-the-law-can-and-cant-do-about-online-harassment/382638/ [https://perma.cc/R6ZW-7URG].

88. *Id.*

89. CITRON, *supra* note 56, at 4 ("The Internet extends the life of destructive posts . . . . Search engines index content on the web and produce it instantaneously. Indexed posts have no built-in expiration date; neither does the suffering they cause. Search engines produce results with links to destructive posts created years earlier.").

90. *Id.* at 10.

91. *Id.*

92. *Id.*

93. *Id.* at 10–11. Other serious conditions that online stalking victims face include posttraumatic stress disorder, eating disorders, depression, and panic attacks. *Id.* at 10.

For example, in a 2010 Wyoming case, a man, posing as his ex-girlfriend on Craigslist and posting an ad requesting a rape scenario, pled guilty to conspiracy to commit sexual assault and other felonies after the ad led his ex-girlfriend to be brutally raped by a man responding to the ad.[94] The ex-boyfriend, Jebidiah Stipe, had previously impersonated several other women on the Internet.[95] The ad, which read in part "[n]eed a real aggressive man with no concerns for women [sic] well being interested let me know," caused the victim's rapist to contact Stipe.[96] Over the course of the several days preceding the rape, the rapist communicated with Stipe—whom he believed was actually the woman requesting the encounter—in an intensely sexual manner, being encouraged to carry out the rape fantasy.[97] Stipe further supplied the rapist with the victim's address, allowing the crime to take place; all of this was done without the victim's knowledge or consent.[98]

Website operators are in a unique position to prevent the harms seen in these cases caused by undesirable digital behavior.[99] "Because site operators control content appearing on their sites, they can minimize the harm by removing or de-indexing abuse before it spreads all over the Internet. They can moderate discussion, adopt clear guidelines for users, and suspend users' privileges if they harass others."[100] Furthermore, because website operators are not state actors, their monitoring is significantly less restrained by the First Amendment.[101] However, due to current immunity extended to website operators, very few incentives to actively monitor and remove harmful content currently exist.

## II. A LACK OF INCENTIVES

Unfortunately, the existing laws and procedures do not adequately address the problem of online impersonation, and

94. William Browning, *2 Plead Guilty in Craigslist Rape Case*, BILLINGS GAZETTE (May 14, 2010), http://billingsgazette.com/news/state-and-regional/wyoming/plead-guilty-in-craigslist-rape-case/article_f1196154-5f0e-11df-820f-001cc4c002e0.html [https://perma.cc/CUZ9-5DNN].

95. CITRON, *supra* note 56, at 5.

96. Browning, *supra* note 94.

97. *Id.*

98. *Id.*

99. CITRON, *supra* note 56, at 167.

100. *Id.* at 167–68.

101. *Id.* at 168.

social media networks have little incentive to stop the behavior themselves. First, this Section examines existing policies social networking sites use to curb online impersonation, such as terms of service and self-reporting. This Section then examines the financial disincentives that social networks have to more heavily enforce anti-online impersonation policies, and finally turns to a discussion of the harmful effects of the broad immunities afforded to these networks through Section 230 of the Communications Decency Act.

### *A. Current Social Media Network Policies to Stop Online Impersonation*

Currently, the most popular social networking sites are Facebook, Twitter, and LinkedIn.[102] Instagram, another well-known social media site, is ranked as the seventh most popular.[103] While not exactly considered social media sites, online dating websites are also ripe with opportunities for online impersonation, with some studies showing that 80 percent of online dating profiles have inaccuracies, even with users knowing that the possibility of meeting a match in person means revealing the inaccuracies.[104] In an attempt to make themselves more attractive to potential matches, users might take liberties with their profiles, running the spectrum from lying about their height or weight to using photographs of a completely different person.[105]

102. *Top 15 Most Popular Social Networking Sites, October 2015*, EBIZ MBA, http://www.ebizmba.com/articles/social-networking-websites (last visited Oct. 2, 2015) [https://perma.cc/K67T-282R]. As of the end of the fourth quarter of 2015, Facebook had 1.59 billion active users, *Number of monthly active Facebook users worldwide as of 4th quarter 2015*, STATISTA, http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (last visited Mar. 12, 2016) [https://perma.cc/SD43-5EGU], Twitter had approximately 320 million users as of September 30, 2015, *Twitter Usage: Company Facts*, TWITTER, https://about.twitter.com/company (last updated Dec. 31, 2015) [https://perma.cc/3XSN-EFTU], and LinkedIn had approximately 396 million members as of late 2015, *Number of LinkedIn members from 1st quarter 2009 to 4th quarter 2015*, STATISTA, http://www.statista.com/statistics/274050/quarterly-numbers-of-linkedin-members/ (last visited Mar. 13, 2016) [https://perma.cc/HU5P-ZQKZ].

103. *Id.*

104. *Fact Sheet 37: The Perils and Pitfalls of Online Dating: How to Protect Yourself*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/perils-and-pitfalls-online-dating-how-protect-yourself (last updated Mar. 2015) [https://perma.cc/7YN5-62U3].

105. *Id.*

Most social media sites have some basic prohibitions against online impersonation within their terms of service. Facebook, for instance, prohibits users from using the site to "bully, intimidate, or harass" other users, as well as doing anything "unlawful, misleading, malicious, or discriminatory."[106] Violations of these terms can result in termination of the user's account.[107] Other social media sites have similar provisions.[108] OkCupid, ranked within the "Top 10 of the Best Rated Online Dating Websites and Services" on consumeraffairs.com,[109] similarly forbids users from "us[ing] personal information about other users . . . for any reason without the express prior consent of the user . . . ."[110] Violation of these terms can result in termination of services and potential action by the company.[111] Cyberharassment, cyberbullying, and online impersonation arguably violate all of the above terms of service.[112]

These social media sites have reporting procedures in place to enable users to notify the site of any violations of the terms of service. OkCupid, for example, has an email address for users to report violations.[113] Facebook also has a reporting procedure, including one specifically for online impersonation.[114] Reporting an account means that it is

106. *Statement of Rights and Responsibilities*, FACEBOOK (Jan. 30, 2015), www.facebook.com/legal/terms [https://perma.cc/9KHA-GE7K].

107. *Id.*

108. *See Impersonation Policy*, TWITTER, https://support.twitter.com/articles/18366 (last visited Nov. 14, 2015) [https://perma.cc/Y3GU-6RBE] (stating that impersonation in a "confusing or deceptive manner" may lead to permanent account suspension); *Twitter Terms of Service*, TWITTER (effective May 18, 2015), https://twitter.com/tos?lang=en [https://perma.cc/7QX2-RR8W] (Twitter may suspend or terminate accounts based on violations of terms of service); *see also Terms of Use*, INSTAGRAM (effective Jan. 19, 2013), https://help.instagram.com/478745558852511 [https://perma.cc/QEQ3-MFVM] (stating users must not "defame, stalk, bully, abuse, harass, threaten, impersonate, or intimidate people or entities"; violations may result in termination of the account).

109. Mark Brooks, *Compare Reviews for Online Dating Sites and Services*, CONSUMER AFFAIRS, http://www.consumeraffairs.com/dating_services/#compare (last visited Oct. 3, 2015) [https://perma.cc/TTG2-QXXR].

110. *Legal Information*, OKCUPID, https://www.okcupid.com/legal/terms (last updated Apr. 24, 2014) [https://perma.cc/T4QH-DRHZ].

111. *Id.*

112. For definitions on these various problematic cyberbehaviors, see *supra* Section I.A.

113. *Legal Information: Safety Tips*, OKCUPID (2015), https://www.okcupid.com/legal/safety-tips [https://perma.cc/5DUE-K58V].

114. *Help Center: Report Something*, FACEBOOK (2015), https://www.facebook.com/help/263149623790594/ [https://perma.cc/GW76-D3V4].

reviewed by Facebook, but the account will not be removed unless it is found to be in violation of the terms of service.[115] Users are able to view their reports and the status of them by visiting their "Support Inbox."[116]

However, even with these policies and procedures in place, users of social media and online dating sites are at risk of cybercrimes, in part because no preemptive measures, other than agreeing to a site's terms of service, exist to prevent impersonators and other would-be harassers from creating fake profiles. In order to create a Facebook account, a person needs only to provide a first and last name, email, and a birthdate; by clicking "sign up," he or she agrees to the terms of service.[117] An essentially infinite number of email addresses can be created; in order to fill out a profile with photographs, an impersonator only needs to find images on Google.[118] Given the difficulty of creating preemptive measures to stop the creation of fake profiles, online impersonation and other cybercrimes cannot be prevented effectively; rather, a site or victim must wait for the problem or violation of the terms of service to actually occur to take action. Moreover, once a fake profile is created, social media networks have little incentive to stop the impersonation.[119] In the meantime, victims suffer the often-damaging consequences of the impersonator's actions.

### *B. Financial Incentives*

Currently, social media networks have little financial incentive to aggressively pursue online impersonators. While the reporting procedures typically allow for termination of accounts for violation of terms of service,[120] this termination

115. *Id.*

116. *Id.*

117. FACEBOOK, www.facebook.com (last visited Mar. 13, 2016) [https://perma.cc/2986-TWWZ].

118. In fact, a simple Google search of "create a fake Facebook page" led to several webpages that included not only basic "how to" steps, but detailed information about how to create a page that "seems real." *See, e.g., How to Create a Fake Facebook Profile*, WIKIHOW, http://www.wikihow.com/Create-a-Fake-Facebook-Profile (last visited Mar 13. 2016) [https://perma.cc/6B5C-2UCR]; *How to Make a Fake Facebook Page Seem Real*, WIKIHOW, http://www.wikihow.com/Make-a-Fake-Facebook-Page-Seem-Real (last visited Mar. 13, 2016) [https://perma.cc/9R6J-3CWU].

119. *See infra* Section II.B, II.C.

120. *See supra* Section II.A.

generally only deletes the offending account; it does not stop an impersonator from creating a different account to continue his or her schemes. Furthermore, social media sites make money by having more monthly users via advertising revenue.[121] The logic is similar to that of television advertising: the more people who watch a show or view a webpage, the more potential customers who at least subconsciously pay attention to a presented advertisement.[122] Facebook estimated that each account generated $5.32 in revenue in 2013.[123] When multiplied by the over one billion active user accounts,[124] it is easy to see how Facebook has become such a successful company.[125] While fake accounts might not be as desirable, they still potentially generate revenue for the site, making aggressive removal policies less enticing to Facebook.[126]

One suggested solution is to change Facebook's financial structure from ad-based to subscription-based revenue.[127] However, if Facebook were to implement this change, thus limiting its dependency on advertising revenue, and arguably enabling it to set more stringent content restrictions, the site would lose a great number of its current users and limit its potential growth.[128] Thus, its current advertiser-supported model is the best way for the site to get more users; and the more users who are on the site, the more advertisers who are

121. Greg McFarlane, *How Facebook, Twitter, Social Media Make Money From You*, INVESTOPEDIA (Sept. 02, 2014), http://www.investopedia.com/stock-analysis/032114/how-facebook-twitter-social-media-make-money-you-twtr-lnkd-fb-goog.aspx [https://perma.cc/MW2N-CDY8].

122. *Id.*

123. *Id.*

124. *Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2015*, *supra* note 102.

125. McFarlane, *supra* note 121.

126. Clanton, *supra* note 38, at 327. One suggested strategy for stopping fake profiles, as well as other undesirable "social spam" like clickbaiting and malicious links, is to require phone verification for accounts. Jamie Tolentino, *5 Types of Social Spam (and How to Prevent Them)*, NEXT WEB, http://thenextweb.com/future-of-communications/2015/04/06/5-types-of-social-spam-and-how-to-prevent-them/#gref (last visited July 3, 2016) [https://perma.cc/6ZUG-JWUF]. Though this solution could curb the creation of fake profiles not linked to any particular user, only seriously monitoring account creation from one IP address—which Facebook currently has the ability to do—can stop a single person from creating multiple accounts. *See How Can I Block Someone by their IP Address?*, FACEBOOK: HELP CENTER, https://www.facebook.com/help/community/question/?id=770029116418579 (last visited July 3, 2016) [https://perma.cc/X4JK-VDFD].

127. McFarlane, *supra* note 121.

128. *Id.*

interested in buying space, and the more money advertisers want to spend to do so—ultimately increasing Facebook's revenue.[129] In order to incentivize website operators to remove harassing content, then, the financial incentive to keep harmful accounts active would have to be removed.

### *C. Section 230 of the Communications Decency Act*

In addition to the financial incentives of keeping fake profiles active, social media networks are afforded broad immunity for the harmful content generated by their users through Section 230. Congress passed the Act in 1996 in response to two court cases discussing the difference between a "distributor" and a "publisher," overruling one of them.[130] A publisher is someone who exercises editorial control over content; a distributor makes the content available to the public without this editorial control.[131] Under the law in most states, a publisher is strictly liable for defamatory statements, while a distributor is liable only for content it knew or should have known was defamatory.[132]

Prior to the passage of the Act, courts were split on whether Internet service providers (ISP), including websites, should be considered publishers or distributors.[133] In *Cubby, Inc. v. CompuServ, Inc.*, Judge Leisure of the Southern District of New York determined that a website that provided its users with a compilation of news sources put together by a third party was only a distributor of information and could not be held liable for defamatory statements contained in the news sources unless there was evidence showing that it knew or should have known of the specific defamatory material.[134] In contrast, the New York Superior Court in *Stratton Oakmont, Inc. v. Prodigy Services Co.* distinguished *Cubby* and held that Prodigy, an interactive computer service,[135] was liable for

129. *Id.*

130. H.R. Conf. Rep. No. 104-458, at 193–94 (1996); Joseph Monaghan, Comment, *Social Networking Websites' Liability for User Illegality*, 21 SETON HALL J. SPORTS & ENT. L. 499, 503 (2011).

131. Monaghan, *supra* note 130, at 503.

132. *Id.* The enactment of Section 230 was meant to overrule this state-level common-law distinction on the national level. *Id.*

133. RICHARD A. EPSTEIN & CATHERINE M. SHARKEY, CASES AND MATERIALS ON TORTS 1031 (10th ed. 2012).

134. 776 F. Supp. 135 (S.D.N.Y. 1991); Epstein, *supra* note 133, at 1031.

135. Section 230(f)(2) defines "Interactive computer service" as "any

defamatory messages published on its bulletin boards because it both advertised that it monitored the posts on its boards and actively screened and edited the messages.[136] Under this holding, "computer service providers who regulated the dissemination of offensive material on their services risked subjecting themselves to liability, because such regulation cast the service provider in the role of a publisher."[137] Congress passed Section 230 a year later to remove the liability created by the *Stratton* decision.[138]

Congress intended Section 230 "to promote the free exchange of information and ideas over the Internet and to encourage voluntary monitoring for offensive or obscene material."[139] Section 230 states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[140] Furthermore, though website operators are statutorily obligated only to provide notice to parents about the availability of parental control software,[141] the statute says nothing about the potential for other abuses.

Additionally, Congress enacted Section 230 to remove any potential disincentives to self-regulation.[142] Post-*Stratton*, fearing that the "specter of . . . liability" imposed by holding interactive computer services liable as publishers would chill any self-regulation by ISP, Congress granted broad immunity in Section 230 and forbid the imposition of publisher liability.[143]

information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." This definition encompasses any person who provides a website that allows users to post their own material, such as blogging platforms, message boards, and social networking sites. *Liability Protections for Online Service Providers under the DMCA and CDA*, BEA & VANDENBERK, http://www.beavandenberk.com/ip/copyright-tm/liability-protections-for-online-service-providers-under-the-dmca-and-cda/ [https://perma.cc/3K3F-7ASB].

136. 1995 WL 323710, at *5 (N.Y. Sup. Ct. May 24, 1995).

137. Zeran v. America Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).

138. EPSTEIN & SHARKEY, *supra* note 133, at 1031.

139. Monaghan, *supra* note 130, at 504; *see also* 47 U.S.C. § 230 (2006).

140. 47 U.S.C. § 230(c)(1) (2012).

141. *Id.* § 230(d).

142. 47 U.S.C. § 230(b)(4) (2006).

143. Zeran v. America Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997); *see* 47 U.S.C. § 230.

Section 230 expressly grants immunity only to interactive computer services as publishers;[144] arguably, under the statutory language, these website operators could still be liable as distributors if they know or have reason to know that the information posted on their site is harmful. However, in *Zeran v. America Online, Inc.*, the Fourth Circuit held that Section 230's immunity extended to America Online for defamatory material posted about the plaintiff on its site, even though America Online had been notified of the material and failed to remove it.[145] Since then, courts in varying circuits have upheld this broad grant of immunity, even in the face of significant harms suffered by plaintiffs and websites operators' knowledge of the harmful material.

For example, in *Ben Ezra, Weinstein, & Co. v. America Online, Inc.*, the Tenth Circuit upheld Section 230 immunity for America Online as an ISP, even though it was acting essentially as a distributor by providing content gathered from other sources.[146] In that case, America Online utilized independent third-party content providers to obtain stock quotation information.[147] The court found that America Online was not liable for the false stock information provided to it by these third parties, despite the fact that it had worked with the third parties to ensure accuracy in previous stock information.[148] The court further concluded that, "Congress clearly enacted [Section] 230 to forbid the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions."[149] Because America Online did not create the information at issue, it was not liable for any defamatory content.[150]

This immunity has been further expanded to encompass harmful online impersonation. The Ninth Circuit upheld immunity for a dating service website that hosted a false and degrading profile.[151] The impersonator posed as actress

144. 47 U.S.C. § 230(c)(1) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

145. 129 F.3d 327 (4th Cir. 1997); *see also* EPSTEIN & SHARKEY, *supra* note 133, at 1032.

146. 206 F.3d 980, 983 (10th Cir. 2000).

147. *Id.*

148. *Id.* at 985.

149. *Id.* at 986.

150. *Id.*

151. Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1120–21 (9th Cir.

Christianne Carafano[152] and indicated in the false profile that the dater[153] was interested in a "hard and dominant man" with a "strong sexual appetite," and that she "liked sort of being controlled by a man, in and out of bed."[154] The profile further included an email address that ultimately would lead anyone responding to the false profile to Carafano's home address and telephone number.[155] As a result of the false profile, Carafano received numerous sexually explicit phone calls and faxes, one even threatening her son.[156] She felt unsafe in her own home and lived in hotels with her son for several months.[157] Carafano sued Matchmaker.com for invasion of privacy, misappropriation of the right of publicity, defamation, and negligence.[158] The court reasoned that Matchmaker.com could not be liable as an "information content provider" because "no profile has any content until a user actively creates it."[159]

After the passage of Section 230, "[c]ourts have roundly immunized site operators from liability even though they knew or should have known that user-generated content contained defamation, privacy invasions, intentional infliction of emotional distress, and civil rights violations."[160] Though Section 230 immunity does not exempt website operators and users from criminal liability,[161] current efforts at state schemes meant to curtail online impersonation and other undesirable cyber behavior face problems of their own.

## III. THE TROUBLE WITH STATE ENFORCEMENT

In an effort to combat cybercrimes, some states have

2003).

152. Carafano uses the pseudonym "Chase Masterson" in her professional work. She is best known for her work on *Star Trek: Deep Space Nine* and *General Hospital*, though she has appeared in many other television and film roles. *See Chase Masterson: Biography,* IMDB, http://www.imdb.com/name/nm0135895/bio?ref_=nm_ov_bio_sm (last visited Mar. 13, 2016) [https://perma.cc/9SYK-NAQN].

153. Though the false profile never named Carafano, it included pictures of her and listed two of her movies. *Metrosplash.com*, 359 F.3d at 1121.

154. *Id.*

155. *Id.*

156. *Id.* at 1121–22.

157. *Id.* at 1122.

158. *Id.*

159. *Id.* at 1124.

160. CITRON, *supra* note 56, at 171.

161. *Id.* at 172.

enacted criminal statutes aimed at addressing this particular criminal concern.[162] However, gaps in statutory drafting and other enforcement difficulties make these criminal statutes ineffective at deterring and punishing online impersonation.[163] Although potentially viable civil claims exist for victims of online impersonation, private litigation is expensive and often difficult to bring against an online impersonator.[164] This Section first examines several existing state statutes aimed at criminalizing online impersonation as well as the problems that criminal statutes face in general. Next, this Section discusses several possible tort claims, using the Restatement (Second) of Torts, that victims could bring against their impersonators and the reasons why these private claims are not likely to be useful or successful.

### *A. Current State Efforts*

While most states have criminal statutes that could address online impersonation, only Texas, Mississippi, Hawaii, New York, and California have enacted statutes that explicitly refer to it.[165]

Texas's specific online impersonation statute, Section 33.07, makes it a third-degree felony[166] to use the name or persona of another person "without obtaining the other person's consent and with the intent to harm, defraud, intimidate, or threaten any person," to create a social media profile, or to send messages through a social media site, thus directly addressing the common understanding of catfishing.[167] Mississippi adds another requirement in its statute: the impersonator must impersonate "an actual person," arguably

162. *See infra* Section III.A.

163. *See infra* Section III.B.

164. *See infra* Section III.E.

165. *Areas of Practice Information Center, Internet Law: E-Personation*, BERTOLLINI & O'REILLY: NEW YORK LITIGATION LAW FIRM, http://www.avvocatidirittointernazionale.com/Areas-of-Practice/Internet-Law/E-Personation.aspx (last visited Oct. 2, 2015) [https://perma.cc/BZ75-FGZH]. The states that have so far addressed the issue of online impersonation with criminal statutes are Arizona, California, Hawaii, Louisiana, Mississippi, New York, Pennsylvania, Texas, and Washington. Amy Coleman, *Catfish Season*, JURIS: DUQUESNE LAW SCHOOL MAGAZINE (Apr. 19, 2013), http://jurismagazine.com/catfish-season/ [https://perma.cc/58ZY-98P7].

166. TEX. PENAL CODE § 33.07(c) (2015).

167. *Id.* § 33.07(a)(1)–(2).

foreclosing any prosecution for someone creating a completely fictitious profile using random pictures from the Internet, even if it was done with the purpose to harass.[168] The Mississippi statute also provides that "an impersonation is credible if another person would reasonably believe, or did reasonably believe, that the defendant was or is the person who was impersonated," further narrowing the scope of criminal liability.[169]

Some states have allowed for a civil remedy in their criminal statutes. California's criminal statute, for example, provides that "any person who knowingly and without consent credibly impersonates another actual person through or on an Internet Web site or by other electronic means for purposes of harming, intimidating, threatening, or defrauding another person is guilty of a public offense . . . ."[170] The statute expressly gives victims the right to a civil action for compensatory damages—including attorney's fees[171]—and injunctive relief.[172] Similarly, Washington's law allows for a civil claim of invasion of privacy when a person impersonates another actual person without consent and with the intent to harass, threaten, intimidate, etc.[173] Provided that the impersonation caused injury to the actual person, such as financial, professional, or reputational harm,[174] the victim may recover actual damages, injunctive and declaratory relief, and fees and costs.[175]

However, even with the existence of these statutes, online impersonation and its potential harms continue to be a problem, both for the victim who fell for the impersonation and the person whose identity was co-opted.

### *B. Why Criminal Statues are Ineffective*

Online crimes like cyberstalking, cyberharassment, and online impersonation "are relatively new crimes that are not

168. MISS. CODE ANN. § 97-45-33(1) (2015).
169. *Id.* § 97-45-33(2).
170. CAL. PEN. CODE § 528.5(a) (West 2015).
171. *Id.* § 528.5(e); § 502(e)(2).
172. *Id.* § 528.5(e).
173. WASH. REV. CODE § 4.24.790(2)(a)–(c) (2015).
174. *Id.* § 4.24.790(2)(d).
175. *Id.* § 4.24.790(3)(a)–(b).

fully integrated into federal and state laws."[176] While the criminal law can serve as a deterrent to would-be harassers and aid victims who cannot afford to bring a private suit,[177] unfortunately the criminal statutes that exist fail to adequately address the dangers of online impersonation.[178] Criminal statutes fail; they are either overly vague, leaving targeted behavior undefined, or under-inclusive, leaving gaps in the law when legislatures are unable to keep up with the rapid pace of technological advancement.[179] Given the dynamic nature of the Internet, "the more specific the language [in the legislation], the more difficult it may be to prosecute such crimes."[180] Thus, victims of online crimes are often left with inadequate protection from their harassers.[181]

One particular shortcoming of many criminal statutes is the requirement of proving intent.[182] Criminal statutes often require intent to "harass and intimidate," which does not reach those with lesser culpable mental states.[183] Similar to traditional stalking laws, "cyberstalking laws require the stalkers to intend, through their conduct, to place the victims in fear of their safety or for their lives."[184] For example, in the case of the Federal Interstate Stalking Punishment and Prevention Act, courts have interpreted its requirement that the perpetrator intend "to kill, injure . . . or cause substantial emotional distress" to mean that the defendant must have the specific intent to carry out the acts.[185] "Thus, even if the victim experiences severe emotional distress that causes [her] to withdraw from school, work, and society, the claim will fail if it cannot be proven that the perpetrator actually intended to cause distress."[186] Similarly, "the credible threat" requirement in many state statutes and the Interstate Communications Act

176. Cassie Cox, Note, *Protecting Victims of Cyberstalking, Cyberharassment, and Online Impersonation Through Prosecution and Effective Laws*, 54 JURIMETRICS J., 277, 278 (2014).

177. CITRON, *supra* note 56, at 123.

178. Cox, *supra* note 176, at 278.

179. Downs, *supra* note 36.

180. Rodolfo Ramirez, *Online Impersonation: A New Forum for Crime on the Internet*, 27 CRIM. JUST. 6, 11 (Summer 2012).

181. Cox, *supra* note 176, at 278.

182. *Id.* at 286.

183. Downs, *supra* note 36.

184. Cox, *supra* note 176, at 286–87.

185. 18 U.S.C. § 2261A(2)(A) (2012); Cox, *supra* note 176, at 287.

186. Cox, *supra* note 176, at 287.

can derail otherwise meritorious claims lacking this particular element.[187] And even if the perpetrator has the requisite intent, online impersonation criminal statutes require that the impersonator be imitating an actual person, rather than just using a real person's pictures to create a fake online persona.[188]

Additionally, the criminal statutes that allow for civil remedies against an impersonator might provide only for claims brought by the person whose identity was co-opted without his or her consent.[189] This incomplete remedy does not provide any claim for the victim who believed the impersonator's scheme, even though "reasonable belief" is a prerequisite for liability.[190] Thus, victims of many of online impersonation's greatest harms, like cyberbullying or dating scams, are left without recourse.[191]

Current laws also fail to address that cybercrimes disproportionately affect women.[192] Data from Working to Halt Online Abuse shows that 72.5 percent of the individuals reporting cyberharassment from 2000 to 2011 were female.[193] And yet, though many states include criminal sentence enhancers for harassment motivated by bias, these provisions are rarely taken advantage of in cybercrime cases.[194] Utilization of these sentence enhancers would make cybercrimes illegal not just as statutory violations, but as hate crimes and civil rights violations as well.[195] The invocation of "[c]ivil rights laws would redress and punish harms that traditional remedies do not: the denial of one's equal rights to pursue life's important opportunities due to membership in a historically subordinated group."[196]

187. *Id.* at 289.

188. Downs, *supra* note 36.

189. *See* WASH. REV. CODE § 4.24.790(2)(d) ("The impersonation proximately caused injury to the actual person.").

190. *Id.* § 4.24.790(1)(c). Arguably California's statute could leave open the possibility for suit brought by either the person whose identity was used, or the person who believed the impersonation. CAL. PEN. CODE § 528.5(e) ("In addition to any other civil remedy available, *a person* who suffers damage or loss by reason of a violation of subdivision (a) may bring a civil action against the violator . . . .") (emphasis added).

191. *See supra* Section I.B for a discussion on the various harms caused by online impersonation.

192. CITRON, *supra* note 56, at 13.

193. *Id.*

194. Sweeney, *supra* note 87.

195. *Id.*

196. CITRON, *supra* note 56, at 23.

While it might seem that states could take some measures going beyond the limitations of Section 230 to aid in criminal enforcement efforts, state legislatures are also specifically prohibited from attempting to override Section 230 by encouraging monitoring by the website operators themselves. The law provides that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this Section,"[197] effectively limiting a state's enforcement possibilities to the criminal law and to prosecutions against individuals.

### *C. The Benefits of Civil Enforcement*

In addition to addressing the shortcomings of criminal statutes, civil enforcement may carry benefits of its own. These can include bypassing concerns of prosecutorial and legislative overreach and ensuring adequate victim compensation.

Some concerns have been raised that over-criminalization of undesirable online behavior will lead "prosecutors [to] use their discretion to investigate and charge defendants in arbitrary and objectionable ways."[198] For example, it is possible that prosecutors may pursue the victim, rather than the defendant who truly caused the harm, if the victim has done something illegal himself or herself, like accessing the defendant's email to discover what he or she is doing.[199] Furthermore, lawmakers are cautioned to "avoid turning so-called repugnant behavior into crimes."[200] These concerns "seem to stem from the notion that 'distasteful' behavior is not sufficiently harmful to warrant criminalization."[201] While these concerns largely trivialize online harassment,[202] a private remedy through the civil justice system could also bypass them.

Moreover, though criminal enforcement can stop undesirable behavior, it leaves victims without monetary compensation for the harms they have suffered.[203] In fact,

197. 47 U.S.C. § 230(e)(3) (2012).
198. CITRON, *supra* note 56, at 186.
199. *Id.* at 186–87.
200. *Id.* at 188.
201. *Id.*
202. *Id.* at 189.
203. *Tort Law Versus Criminal Law*, ROSS FELLER CASEY, http://www.rossfellercasey.com/newsletters/tort-law-versus-criminal-law/ (last visited June 4, 2016) [https://perma.cc/V54X-V6YL].

"there is an assumption in criminal law that tort law exists to compensate the victim for the victim's financial harm."[204] This financial compensation is relevant in the area of online impersonation, where victims often suffer pecuniary harms in addition to reputational or other harms.[205] Through a private enforcement mechanism, such as civil liability for online impersonation, victims can be fully compensated for their harms while avoiding the pitfalls of ineffective criminal statutes and the public concerns of over-criminalization.

### *D. Potential Civil Causes of Action*

There are possible tort claims that address online impersonation and its harms. In an online impersonation scheme, there are two possible victims: (1) the person whose online persona was stolen and who suffered some sort of reputational harm and (2) the person who believed the impersonator's scheme and suffered some sort of damages as a result.[206] These wrongs can be best addressed by privacy torts and defamation claims for the former plaintiffs, and by fraud and emotional distress claims for the latter. By bringing a private tort claim, plaintiffs will be able to seek damages for the harms caused by impersonators stealing their online personas; though the doctrine of privacy torts is not perfectly suited to the newer realm of Internet impersonation,[207] viable claims do exist. This Section examines several possible general tort claims—misappropriation of likeness, defamation, intentional infliction of emotional distress, and fraudulent misrepresentation—that victims could bring, with the Restatement (Second) of Torts as a guide.[208]

204. *Id.*

205. *See supra* Section I.B. for a discussion on the various harms suffered by victims of online impersonation.

206. *See supra* Section I.B.

207. *See* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1809 (2010) (explaining that while courts have "erected a number of substantial barriers to recovery," online harms are compounded by the permanent and searchable nature of the Internet).

208. Because the specific elements of tort claims vary state to state, this Section will only be a survey of the general aspects of potential claims.

### 1. Misappropriation of Likeness

Misappropriation of likeness is one of the recognized privacy torts.[209] The Restatement (Second) of Torts provides that "[o]ne who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."[210] Though the tort is not specifically meant to apply only to commercial purposes, some states have limited liability to the commercial use of the plaintiff's name or likeness.[211]

In order for a defendant to be liable, "the defendant must have appropriated to his own use or benefit the reputation, prestige, social or commercial standing, public interest or other values of the plaintiff's name or likeness."[212] In cases of online impersonation, the plaintiff would need to show that the defendant appropriated his or her likeness for some benefit, such as to take advantage of an existing relationship, as in the Megan Meier case,[213] or perhaps to fulfill a malicious purpose, such as in the Carafano case.[214]

### 2. Defamation

To maintain a cause of action for defamation, a plaintiff must show that there was: "(a) a false and defamatory statement concerning another; (b) an unprivileged publication to a third party; (c) fault amounting to at least negligence on the part of the publisher; and (d) either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication."[215] Additionally, in the case of private plaintiffs, it is not necessary to demonstrate that actual reputational harm occurred; rather, a statement's defamatory character "depends upon its general tendency to have such an effect."[216]

209. *See* RESTATEMENT (SECOND) OF TORTS § 652C (AM. LAW INST. 1977).

210. *Id.*

211. *Id.* at cmt. b. The states that limit liability to commercial uses are New York, Oklahoma, Utah, and Virginia. *See id.* at Reporter's Note.

212. *Id.* at cmt. c.

213. *See* Wegman, *supra* note 77, at 745–46.

214. *See* Carafano v. Metrosplash.com, Inc., 39 F.3d 1119, 1120–21 (9th Cir. 2003).

215. RESTATEMENT (SECOND) OF TORTS § 558 (AM. LAW INST. 1977).

216. *Id.* § 559 cmt. d; *see also* Dun & Bradstreet v. Greenmoss Builders, Inc., 472 U.S. 749, 760–61 (1985) (awarding presumed damages to a private plaintiff).

A statement is defamatory if it harms the victim's reputation in the community or "deter[s] third persons from associating or dealing with him," thus exposing the victim to "hatred, ridicule, or contempt."[217] The statement may not just be an opinion, as stated by the United States Supreme Court in *Gertz v. Robert Welch, Inc.*: "We begin with the common ground. Under the First Amendment there is no such thing as a false idea. However pernicious an opinion may seem, we depend for its correction not on the conscience of judges and juries but on the competition of other ideas."[218] Rather, the statement may be in the form of an opinion, but must imply the allegation of defamatory facts as its basis.[219]

For victims of online impersonation, a cause of action could lie upon a showing that the fake profile gave information that was false and harmful to the victim's reputation, and that others viewed the fake profile.

### 3. Intentional Infliction of Emotional Distress

An online impersonator is liable for severe emotional distress if he or she causes it by extreme and outrageous conduct.[220] Courts typically find liability only when the defendant's conduct is "so outrageous in character, and so extreme in degree, as to go beyond all possible bounds of decency, and to be regarded as atrocious, and utterly intolerable in a civilized community," rather than "mere insults . . . or other trivialities."[221] Furthermore, the defendant must intend to inflict severe emotional distress and know that such distress is substantially certain to arise from his conduct.[222] The plaintiff must be able to prove the fact of severe emotional distress and that the distress was reasonable and justified given the circumstances.[223]

In extreme cases of online impersonation, such as the Stipe case in Wyoming,[224] a plaintiff whose identity was co-opted could have a viable cause of action for intentional infliction of

217. RESTATEMENT (SECOND) OF TORTS § 559, cmt. b, c. (AM. LAW INST. 1977).
218. 418 U.S. 323, 339–40 (1974).
219. RESTATEMENT (SECOND) OF TORTS § 566 (AM. LAW INST. 1977)
220. *Id.* § 46.
221. *Id.* cmt. d.
222. *Id.* cmt. i.
223. *Id.* cmt. j.
224. *See* Browning, *supra* note 94.

emotional distress. Any plaintiff who believed an impersonator's scheme could also bring a claim for intentional infliction of emotional distress. For example, victims of fraud or extortion at the hands of an impersonator, upon proper proof, could allege these damages.

4. Fraudulent Misrepresentation

Should an online impersonator convince his or her victim to send money or otherwise act in reliance on the impersonator's assertions, the impersonator could be liable for fraudulent misrepresentation. Fraudulent misrepresentation occurs when a person "fraudulently makes a misrepresentation of fact, opinion, intention or law for the purpose of inducing another to act or to refrain from action in reliance upon it."[225] A misrepresentation can be written or spoken words, as well as any other conduct that amounts to an assertion.[226]

A misrepresentation is fraudulent if its maker "knows or believes the matter is not as he represents it to be."[227] Thus, an online impersonator pretending to be someone else falls under this definition. An impersonator is liable only if the victim justifiably relies on the misrepresentation in changing his behavior.[228] However, the impersonator is still liable if the victim could have made an investigation into the truth of the misrepresentation—there is no implied duty to investigate.[229]

Fraudulent misrepresentation can be a particularly attractive remedy for victims who believe an impersonator's scam. They are under no duty to investigate, which, given the relatively anonymous nature of the Internet, means that a victim is not held responsible for his or her failure to discover "the truth."[230] The victim would then be able to recover the money he or she spent in relying on the misrepresentations.[231]

Though tort claims exist that could remedy online impersonation's harms, private litigation poses many additional problems and risks to plaintiffs. This makes it an unrealistic option for being the sole remedy for online

225. RESTATEMENT (SECOND) OF TORTS § 525 (AM. LAW INST. 1977).
226. *Id.* cmt. b.
227. *Id.* § 526.
228. *Id.* § 537.
229. *Id.* § 540.
230. *See infra* Section III.D.
231. RESTATEMENT (SECOND) OF TORTS § 537 (AM. LAW INST. 1977).

impersonation without additional incentives.

### *E. What Problems Might Arise With Private Litigation?*

Private litigation is not without its own flaws, particularly as the law currently stands. Plaintiffs can face potential financial challenges, as well as especially complex cases. These problems are best addressed not by the private litigant, but rather by the party holding the majority of the available information: the network provider.

Litigation is extremely expensive, and many of the victims of online impersonation are young, making it difficult for them to finance a private lawsuit.[232] As any civil claim currently stands, plaintiffs face a likely risk of judgment-proof defendants[233] from whom recovery will be difficult or impossible, making costly litigation not worth the effort. However, by giving victims the opportunity to hold network providers liable in addition to the impersonators, financial compensation is potentially available from both sources, making available damages much more attractive and lucrative—and therefore more enticing.

Furthermore, cybercrimes, including online impersonation, have several unique factors that make them more difficult to detect:

> (1) the anonymous nature of many online activities allows cybercriminals to mask their identities, (2) cybercrimes can be achieved from virtually anywhere in the world, as long as there is Internet access, (3) technology can be used to hide the criminal activity and delay or even prevent the victim from learning of the crime, and (4) the size of the Internet provides an enormous pool of potential victims for these

232. Clanton, *supra* note 38, at 340.

233. A judgment-proof defendant is one who is "unable to satisfy a judgment for money damages because the person has no property, does not own enough property within the court's jurisdiction to satisfy the judgment, or claims the benefit of statutorily exempt property." *Judgment-Proof*, BLACK'S LAW DICTIONARY (10th ed. 2014). The term is most commonly used in tort and contract law to describe defendants or potential defendants who are financially insolvent. *Judgment Proof*, WIKIPEDIA, https://en.wikipedia.org/wiki/Judgment_proof (last visited June 4, 2016) [https://perma.cc/U5Y9-KKBS].

crimes.[234]

These unique problems mean that for a victim of online impersonation, it is more difficult to detect the unwanted behavior, identify who is to blame, and follow through with a cause of action.[235]

However, problems of anonymity and other difficulties can be addressed by the entity who holds the account information—the website operator. These website operators also have significant resources at their disposal, making the responsibility of investigation of harmful accounts most efficiently handled by them.[236] The only way to spur website operators to take up this responsibility is to address the problem of online impersonation on a national scale.

## IV. A NATIONAL ISSUE

Given the difficulty posed by both state criminal statutes and current private tort actions, online impersonation, and the host of associated problems, is truly an area best addressed by federal law. Because federal law is uniform and backed by federal enforcement agencies, the problems of varying availability of enforcement that stem from state statutory remedies can be bypassed.[237] It is largely the result of Section 230, part of a federal statute itself, that online impersonation is able to flourish relatively unchecked. However, federal law already addresses a similar problem in the Digital Millennium Copyright Act.[238] By applying the principles of the enforcement scheme of the Digital Millennium Copyright Act to Section 230, via an amendment to the statute, federal law will be able to more adequately address the harms caused by online

234. Michael D. Scott, SCOTT ON INFORMATION TECHNOLOGY § 17.11 (Aspen Pub. ed., 3d ed. 2014).

235. *Id.* ("Many crimes committed online are merely a variation of their offline brethren. However, these online crimes are more difficult to detect, identify the perpetrator, and to apprehend and try the criminal.").

236. Although there are some potential arguments against subjecting social networking sites to more civil liability, these problems are outweighed by the benefits of creating a safer online community, particularly given that the narrow construction of waiving of immunity, as has been the case in the Digital Millennium Copyright Act, means that social networks would face civil liability only in the most severe cases. *See infra* Sections IV.C, IV.E.

237. *See supra* Sections III.A, III.B.

238. *See infra* Section IV.C.

impersonation.

This Section examines the existing federal laws that address cybercrimes, as well as their shortcomings. It then outlines why the Communications Decency Act is ripe for amendment and looks to the Copyright Act as a model for an enforcement scheme. Finally, this Section proposes an amendment to Section 230 of the Communications Decency Act.

### *A. What Existing Federal Laws Address Cybercrimes?*

Federal law encompasses a wide swath of undesirable online conduct;[239] however, to date, there are no federal online impersonation statutes.[240] Nevertheless, depending on the behavior and its effect, victims of cybercrimes and online impersonation may be able to bring charges under federal law.

One applicable statute is the Interstate Communications Act.[241] This law criminalizes any threats "to injure the person of another."[242] Thus, only cyberharassment that escalates to credible threats can be prosecuted. Similarly, the Federal Interstate Stalking Punishment and Prevention Act prohibits someone who has the "intent to kill, injure, harass, or intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person" from using "the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce" to engage in a course of conduct that places the person in reasonable fear of death or serious bodily injury or that "causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress."[243] There is no requirement of a direct threat to the victim,[244] encompassing a broader range of conduct than the Interstate Communications Act. Federal prosecutors can also

239. CITRON, *supra* note 56, at 124. This conduct includes cyberstalking, threatening and harassing an individual over interstate communication networks, soliciting a stranger to attack or stalk another, hacking, and perpetrating identity theft. *Id.* at 124–25.

240. BERTOLLINI & O'REILLY: NEW YORK LITIGATION LAW FIRM, *supra* note 165.

241. 18 U.S.C. § 875 (2012).

242. *Id.* § 875(c).

243. 18 U.S.C.A. § 2261A(2)(A)–(B) (West 2013).

244. Cox, *supra* note 176, at 282.

bring charges under the Telephone Harassment Act, which was amended in 2006 to include electronic communications or, in cases involving solicitation of minors, the Child Protection and Sexual Predator Punishment Act.[245] Federal prosecutors have attempted to bring cases under the Stored Communications Act, as well as the Computer Fraud and Abuse Act; however, courts have refused to apply these statutes to online impersonation and harassment.[246]

In 2009, following the aftermath of the Megan Meier case, Congresswoman Linda Sanchez introduced the Megan Meier Cyberbullying Prevention Act.[247] The bill, designed to prohibit the use of electronic means "with the intent to coerce, harass, or cause substantial emotional distress to a person . . . to support severe, repeated, and hostile behavior,"[248] was met with concerns about broad over-criminalization and First Amendment infringement.[249] The bill was heard in the House Subcommittee on Crime, Terrorism, and Homeland Security in September 2009, but nothing has happened since.[250]

245. *Id.* at 287; 47 U.S.C. § 223(a)(1)(C) (2012) ("Whoever . . . in interstate or foreign communications . . . makes a telephone call or utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any specific person."); 18 U.S.C. § 2425 (2012) ("Whoever, using the mail or any facility or means of interstate or foreign commerce . . . knowingly initiates the transmission of the name, address, telephone number, social security number, or electronic mail address of another individual, knowing that such other individual has not attained the age of 16 years, with the intent to entice, encourage, offer, or solicit any person to engage in any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title, imprisoned not more than 5 years, or both.").

246. 18 U.S.C.A. §§ 2701–12 (West 2015); 18 U.S.C. § 1030 (2012); *see* Doe v. Hofstetter, No. 11-cv-02209-DME-MJW, 2012 WL 2319052 (D. Colo. June 13, 2012) (using a fake Twitter account to distribute illicit photographs of plaintiff was not a violation of anti-hacking statutes, even if the account was created in violation of Twitter's terms of service). For further discussion on claims under the anti-hacking statutes, see Richard Raysman & Peter Brown, *Online Impersonation Continues, with Varying Consequences,* N.Y. L.J. (Aug. 11, 2015), http://www.newyorklawjournal.com/id=1202734353364/Online-Impersonation-Continues-With-Varying-Consequences [https://perma.cc/PM3Y-V2VX].

247. H.R. 1966, 11th Cong. (2009), https://www.congress.gov/bill/111th-congress/house-bill/1966/text [https://perma.cc/TUN6-7NXG]; David Kravets, *Cyberbullying Bill Gets Chilly Reception*, WIRED (Sept. 30, 2009), http://www.wired.com/2009/09/cyberbullyingbill/ [https://perma.cc/LM62-R9JE].

248. H.R. 1966; Kravets, *supra* note 247.

249. Kravets, *supra* note 247.

250. *Comms.: H.R. 1966 – Megan Meier Cyberbullying Prevention Act*, CONGRESS.GOV, https://www.congress.gov/bill/111th-congress/house-bill/1966 (last visited Mar. 12, 2015) [https://perma.cc/8CCN-XC3E].

Because current efforts are not working or are standing still, the time is ripe for Congress to act by amending Section 230.

### *B. A Need for Change Within Section 230*

Congress's broad grant of immunity to online content providers, including social media networks, via Section 230 allows online impersonators to flourish for two reasons. First, there is a lack of liability on the network's part that reduces its incentive to research and remove harmful content. Second, without a "deep pocket" from which to recover, plaintiffs with viable claims are less likely to bring suit, thereby weakening any deterrent effect civil causes of action might have on impersonators.

In 1996, at the time of the Communication Decency Act's enactment, the Internet was a vastly different space than it is now.[251] ISPs began to realize that they could profit from providing online content in addition to Internet services.[252] However, the immunity granted to these companies remained the same as ISPs expanded their role from service providers to content providers.[253] "It is uncertain whether Congress would have afforded the same protection at the time it enacted the CDA had it known that ISPs would deliver content in the future."[254]

Furthermore, the way Internet users create and interact with online content has undergone tremendous changes from 1996 to the present. The revolution of "Web 2.0" applications, which allow users to dialogue with one another in a virtual community, has led Internet users away from passive viewing

251. Monaghan, *supra* note 130, at 505.

252. *Id.*

253. *Id.*; *see, e.g.*, Dimeo v. Max, 433 F. Supp. 2d 523 (E.D. Pa. 2006) (finding no liability for host of message board for defamatory posts); Universal Commc'n. Sys. v. Lycos, Inc., 478 F.3d 413, 419 (1st Cir. 2007) (holding that website operators are providers of interactive computer services within the meaning of Section 230 because the website "enables computer access by multiple users to [a] computer server"); Goddard v. Google, C 08-2738 JF, 2008 U.S. Dist. LEXIS 101890, at *9 (N.D. Cal. Dec. 17, 2008) (holding that merely providing third parties with tools to create web content is immunized by Section 230). "Moreover, even if a service provider knows that third parties are using such tools to create illegal content, the service provider's failure to intervene is immunized." *Id.*

254. Monaghan, *supra* note 130, at 505.

of content to dynamic creation.[255] Though it is difficult to pinpoint precisely when the Web 2.0 revolution occurred, the term was coined in 1999 and was popularized at the O'Reilly Media Web Conference in late 2004.[256] Regardless of the exact "start" date of Web 2.0, it is reasonable to assume that Congress did not contemplate the interactive, dynamic Internet of the present day when it enacted the Communications Decency Act.

A look into the legislative history of the Act illustrates this point. Section 230(a)(4) states: "[t]he Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation," illustrating Congress's commitment to allowing the Internet to remain a space for free public discourse.[257] The policy behind the statute is further elaborated:

> It is the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulations; encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services; [and] to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material . . . .[258]

By focusing on "the vibrant and competitive free market" and maximum "user control,"[259] Congress chose to favor the

255. Tim O'Reilly, *What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software,* O'REILLY (Sept. 30, 2005), http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html [https://perma.cc/6HLB-TA4C].

256. *Web 2.0,* WIKIPEDIA, https://en.wikipedia.org/wiki/Web_2.0 (last visited Mar. 13, 2016) [https://perma.cc/5ZTH-TVM7].

257. This passage was quoted with favor by the court in *Zeran v. America Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997). The court reasoned that, based on this congressional commitment, "[t]he specter of tort liability in an area of such prolific speech would have an obvious chilling effect," thus supporting its conclusion in favor of broad immunity for ISPs. *Id.* at 331.

258. 47 U.S.C. § 230(b)(2)–(4) (2012).

259. *Id.*

proliferation of free speech over deterrence of potentially harmful speech.

The current system Congress envisioned has allowed harmful online behavior to proliferate alongside free speech.[260] As a result of the Web 2.0 revolution, users of interactive web services have much more control over the content they create—far more than they had in 1996, or even when earlier cases were being decided.[261] While a great deal of this user autonomy has created beneficial online content, some of it has also led to dangerous, damaging scenarios, such as Megan Meier's suicide.[262] Therefore, in order to lessen these harmful effects, Congress should decrease the broad immunity granted to social networking sites, holding them liable under a "distributor" theory, as opposed to the broad immunity they currently enjoy.[263]

Section 230(c) already provides for "[p]rotection for 'Good Samaritan' blocking and screening of offensive material," stating that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[264] "Publisher" or "speaker" takes language directly from defamation law.[265] Traditional defamation law also recognizes a third type of liability: distributor liability, which imposes liability for the republication or distribution of defamatory statements only if the party, such as a bookseller or news vendor, knew or should have known about the defamation.[266] Courts have acknowledged that while

260. *See supra* Part I.

261. The core competencies of Web 2.0 Companies, as defined by Tim O'Reilly, illustrate this point. Successful Web 2.0 companies emphasize, among other competencies: "(1) services, not packaged software, with cost-effective scalability, (2) control over unique, hard-to-recreate data sources that get richer as more people use them, (3) trusting users as co-developers, [and] (4) harnessing collective intelligence . . . ." O'Reilly, *supra* note 255.

262. *See supra* Section I.B.2.

263. *See supra* Section II.C.

264. 47 U.S.C. § 230(c)(1) (2012).

265. Section 558 of the Restatement (Second) of Torts lists the elements of a cause of action for defamation as: "(a) a false and defamatory statement concerning another; (b) an unprivileged publication to a third party; (c) fault amounting at least to negligence on the part of the publisher; and (d) either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication." RESTATEMENT (SECOND) OF TORTS, *supra* note 215.

266. *See, e.g.*, Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 139 (S.D.N.Y.

distributor liability could exist for website operators, this has been overridden by Congress's grant of immunity in Section 230.[267] However, in light of the changing face of the Internet and the damaging effects of online impersonation and other harmful digital conduct, distributor liability for social media sites and other website hosts needs to be implemented.

Under a theory of distributor liability, a social networking site would be held responsible for content that it knew or should have known was harmful.[268] This means that a site would be responsible for investigating, removing, and preventing further harm from deceptive profiles that are reported using the site's reporting procedures. This, in turn, would allow citizens to bring actions not just against their online harassers, who may or may not be identifiable or financially solvent, but also the social media sites that allowed the harm to occur. A similar liability structure already exists for copyright-infringing material under the Digital Millennium Copyright Act.

### *C. The Digital Millennium Copyright Act*

The Digital Millennium Copyright Act, enacted in 1998, exemplifies how a website operator can be afforded broad immunity while still being liable for the known harms that it fails to prevent.[269] Section 512 of the Act generally grants immunity to website operators for copyright-infringing material, provided that the material was not created by the website operator itself[270]—similar to the grant of immunity in Section 230 of the Communications Decency Act. However, this immunity is subject to several limitations: (1) the ISP must not have actual knowledge of the infringing material or, in the absence of actual knowledge, is not aware of facts or

1991) (defining distributor liability under New York law).

267. *See* Blumenthal v. Drudge, 992 F. Supp. 44, 51–52 (D.D.C. 1998) (declining to hold AOL liable for a defamatory gossip column posted on its webpage due to Section 230, but recognizing that "[b]ecause [AOL] has the right to exercise editorial control over those with whom it contracts and whose words it disseminates, it would seem only fair to hold AOL to the liability standard applied to a publisher, or at least, like a book store owner or library, to the liability standards applied to a distributor").

268. Monaghan, *supra* note 130, at 503.

269. Pub. L. No. 105-304 (codified as amended in scattered sections of 17 U.S.C. and 28 U.S.C.).

270. 17 U.S.C. § 512(c)(1) (2012).

circumstances from which infringing activity is apparent (the "red flag" provision);[271] (2) the ISP must "act expeditiously" to remove the infringing material once it has knowledge of the infringing material's existence;[272] and (3) the ISP must not receive a financial benefit from the infringing material.[273]

Thus, an ISP becomes liable for removing copyright-infringing material once it has adequate notice of said material.[274] Furthermore, to aid in identifying infringing material, the statute allows a copyright owner to subpoena a service provider for an alleged infringer's identity.[275] Should a service provider fail to comply with the removal provisions of the statute, a complaining party may be able to get either monetary damages or injunctive relief from the service provider—even for content the provider itself did not create.[276]

Courts have narrowly construed this waiver of immunity. The Southern District of New York in *Viacom International, Inc. v. YouTube, Inc.* found that the Digital Millennium Copyright Act protected YouTube when it removed infringing material upon receiving notice of the material and thus awarded summary judgment.[277] On appeal, the Second Circuit construed Section 512(c)(1)(A)(ii), the so-called "red flag" provision, as requiring that the "facts or circumstances" that would make infringing content apparent be considered under an objective standard.[278] That is, the red flag provision "turns on whether the provider was subjectively aware of facts that would have made the specific infringement 'objectively' obvious to a reasonable person."[279]

271. *Id.* §§ 512(c)(1)(A)(i)–(ii); Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2d Cir. 2012).

272. 17 U.S.C. § 512(c)(1)(A)(iii).

273. *Id.* § 512(c)(1)(B).

274. *Id.* Sections 512(c)(3)(A)(i)–(vi) define adequate notice as a written communication that identifies the infringing material, its location, a way to contact the complaining party, and includes a statement that the party believes in "good faith" that the material is infringing.

275. *Id.* § 512(h)(1).

276. *Id.* §§ 512(a)–(j).

277. 718 F. Supp. 2d 514, 526 (S.D.N.Y. 2010).

278. 676 F.3d 19, 31 (2d Cir. 2012).

279. *Id.* Because the district court did not consider YouTube's knowledge of several infringing clips, either whether it had actual knowledge or the objective "red flag" knowledge, the court remanded for further proceedings. *Id.* at 34. On remand, the district court was also asked to consider whether YouTube was "willfully blind" to infringing content, though the Second Circuit was careful to condition this inquiry with the warning that there is no duty for any internet

This same "red flag" provision, which holds ISPs liable for copyright-infringing material of which they have notice, could be utilized for holding social networking sites liable for harmful content under the same "objectively obvious to a reasonable person" standard.[280] However, this requires an amendment to Section 230.

### *D. A Proposed Amendment*

In order to encourage responsible monitoring practices by website hosts, as well as deter individuals from undesirable online behavior, Section 230 of the Communications Decency Act must be amended. Using the model provided by Section 512(c) of the Digital Millennium Copyright Act, the immunity granted to website operators should be conditioned on their "expeditious removal" of harmful content, making website operators liable as distributors of known harmful material if they do not remove said content.

This liability could be implemented by amending Section 230(c) to read as follows[281]:

> (1) Treatment of publisher or speaker. No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider, *unless that information is (1) harmful, defamatory, or meant to otherwise harass and (2) the provider had actual knowledge of the nature of the information or, in the absence of such actual knowledge, is aware of facts or circumstances that would make the harmful, defamatory, or otherwise harassing nature of the information apparent, and failed to expeditiously remove the harmful content.*

service provider to "affirmatively monitor" for infringing content. *Id.* at 35. At the conclusion of the remanded proceedings, the district court found that YouTube lacked any specific knowledge of the infringing material, largely because Viacom was not able to prove that they *had* knowledge. Viacom Int'l, Inc. v. YouTube, Inc., 940 F. Supp. 2d 110, 116 (S.D.N.Y. 2014). Thus, the court determined YouTube was still protected by the safe-harbor immunity of Section 512 of the Digital Millennium Copyright Act. *Id.* at 123.

280. *Viacom*, 676 F.3d at 31.

281. Italicized text identifies the amended text. Proposed section (c)(2) would appear before the existing section (c)(2), which would become (c)(3). *See* 47 U.S.C. § 230(c) (2012).

> (2) *Should a provider of an interactive computer service fail to expeditiously remove harmful content of which it had actual or constructive notice, as defined above, it becomes liable as a distributor of the harmful content and subject to civil suit, subject to the damages provided for in section 206 of this Act.*[282]

This amendment would enable private citizens to hold websites responsible for any known damaging content posted on the site.

Limiting the liability to scenarios in which the website provider has actual knowledge, or should have had knowledge, of the content is beneficial for two reasons. First, it eliminates concerns over website operators needing to over-restrict or monitor their sites. Courts have been concerned with placing too high a regulatory burden on website operators, reasoning that the threat of litigation from a failure to monitor millions of users and their content is far too onerous.[283] However, most social media networks have reporting procedures in place, aimed at encouraging users to self-police for harmful content.[284] Under this proposed amendment, a social media network would not face liability for harmful content until it receives a report from a user or notices other problems consistent with online harassment.

Second, this limited liability addresses concerns about needless litigation, or people suing over mere hurt feelings. Though it is likely that users of social media over-report harmful postings, the networks respond by investigating the posts to determine whether they are harmful or not. The added distributor liability for knowledge of actually harmful posts incentivizes networks to diligently look into these posts and communicate with the reporter to try to curtail any undesirable behavior, particularly given the financial incentives social

282. 47 U.S.C. § 206 allows for common carriers in violation of the Act to be held liable "for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter, together with a reasonable counsel or attorney's fee."

283. *See* Zeran v. America Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997) ("It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted.").

284. *See supra* Section II.A.

media networks currently have to generate and keep as many users as possible.[285] The network can also communicate with the reporter, as many already do, to let the reporter know that the content was not actually in violation of any terms of service.[286]

### *E. Potential Problems with an Amendment*

An enforcement scheme structured around notice, as this amendment proposes, could be problematic. However, these problems are easily resolved, and the amendment is the best possible solution.

For example, one of the current criticisms of existing copyright law is that it is too difficult and expensive for individuals to enforce their intellectual property rights.[287] The Digital Millennium Copyright Act allows for copyright holders to send a Digital Millennium Copyright Act notice, a sort of cease-and-desist letter, to website operators informing them that one of the site users is committing copyright infringement.[288] However, because enforcement of copyright laws can be expensive and time consuming, "gray-area or even illegal creativity" go unpunished, even with this notice provision in place.[289] In contrast to investigating and enforcing one's intellectual property rights, which can be complicated and perhaps require the assistance of counsel, knowing whether a fake profile is harassing or otherwise harmful is largely a matter of the victim's subjective interpretation, therefore enabling the victim to independently decide to report the conduct with little assistance. Furthermore, social media networks already have reporting schemes in place that are designed to be user-friendly and low-cost.[290] Through this

285. *See supra* Section II.B.

286. For example, Facebook has a "Support Inbox" feature that allows a user to see what action has been taken on any reports that the user has made. *Can I Check the Status of Something I've Reported to Facebook?*, FACEBOOK: HELP CENTER, https://www.facebook.com/help/338745752851127 (last visited Mar. 12, 2015) [https://perma.cc/2SH4-M9B7].

287. *What Are the Major Criticisms of the Copyright Laws in the US?*, NEW MEDIA RIGHTS (Nov. 25, 2011, 3:05 PM), http://www.newmediarights.org/business_models/artist/what_are_major_criticisms_copyright_laws_us [https://perma.cc/CA6U-TKF3].

288. *Id.*; 17 U.S.C. § 512(c)(3) (2012).

289. *What Are the Major Criticisms of the Copyright Laws*, *supra* note 287.

290. *See supra* Section II.A.

existing notice scheme, users will be able to enforce their personal rights to privacy and safety with little complication.

Additionally, there could be potential problems with this amendment to Section 230 restricting Internet users' right to free speech. However, "the Court has never held that criminal libel law is unconstitutional, and indeed it continues to be used in some states."[291] There are distinctions in the varying standards of liability in defamation law, turning on the status of the plaintiff and defendant. While defamation law is largely protective of media defendants,[292] the liability standard for private defendants, such as individuals, speaking about private plaintiffs, or those who are not public figures who "command[] a substantial amount of independent public interest,"[293] continues to be the lower negligence standard.[294] Though this proposed amendment to Section 230 could implicate public plaintiffs and defendants, it will most likely encompass disputes between private individuals. The same argument for less stringent First Amendment protections that has been made in defamation cases could apply in these circumstances as well, given that no heightened standard of liability applies to private individuals.

Thus, though there could be some problems with amending Section 230, these problems are largely avoided given the context of the amendment and existing case law and are outweighed by the importance of deterring harmful cyber behavior to create a safer Internet for all.

291. Eugene Volokh, *Impersonating Someone Online with Intent to Injure His Reputation is a Crime in New York*, VOLOKH CONSPIRACY (May 13, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/05/13/impersonating-someone-online-with-intent-to-injure-his-reputation-is-a-crime-in-new-york/ [https://perma.cc/T7FL-9PKL].

292. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279–81 (1964) (adopting the rule that a public figure may not recover damages from media defendant for a defamatory falsehood unless the statement was made with "actual malice," or "knowledge that it was false or with reckless disregard of whether it was false or not," largely for the purpose of protecting the First Amendment right to freedom of the press).

293. Curtis Pub. Co. v. Butts, 388 U.S. 130, 154 (1967) (holding that the "actual malice" standard applies not just to public officials, but to public figures as well).

294. *See* Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 760–61 (1985) (finding that because defamation suits between private parties do not pose a "threat to the free and robust debate of public issues," less stringent First Amendment protections are appropriate).

## CONCLUSION

Online impersonation presents a unique set of harms to its victims. Those whose online personas are stolen by an impersonator can face reputational damage, loss of business opportunities, and emotional distress. Those who are duped by an impersonator can experience severe financial loss and emotional anguish upon learning a relationship was fabricated. Unfortunately, the current state of the law leaves many of these victims without compensation for the harms they suffer. By limiting social media networks' immunity under Section 230, website operators are given an incentive to more carefully monitor reported harmful content, and victims are given a more viable remedy should a website operator fail to do so.

For example, consider the case of Chris Andersen, the NBA player whose career was seriously damaged by an online impersonation. Under the current regime, he could try to bring suit against his impersonator, Shelly Lynn Chartier; however, like in most catfishing schemes, his impersonator—who has been described as a recluse who "live[s] in filth"—is probably judgment proof.[295] Thus, it is likely that, even if Andersen were to prevail on a private claim against Chartier, he would be unable to collect any monetary damages from her, and he would be unable to sue any of the social media platforms through which the two communicated. And though Chartier was eventually prosecuted for and convicted of several charges relating to her multiple complex online schemes, these criminal convictions in Canada leave Andersen with no compensation for the damage to his reputation and the millions he lost in sponsorship deals.[296]

However, under this proposed amendment, Andersen would have been able to bring a claim for defamation,[297]

295. Joel Christopher, *Cunning Celeb-Obsessed Recluse Who Impersonated NBA Star AND a 17-year-old Girl on Facebook, Set Them Up to Have Sex and Then Blackmailed Him Is in Jail,* DAILYMAIL.COM (Oct. 30, 2015, 7:38 am), http://www.dailymail.co.uk/news/article-3295556/Agraphobic-Canadian-woman-catfished-NBA-star-Chris-Birdman-Andersen-online-sentenced-18-months-jail.html [https://perma.cc/A5FD-FGHJ].

296. Mike McIntyre, *How a Reclusive Woman in Rural Manitoba Scammed an NBA Star,* WINNIPEG FREE PRESS: IN CASE YOU MISSED IT (Aug. 20, 2015, 6:55 pm), http://www.winnipegfreepress.com/special/in-case-you-missed-it/How-a--recluse-woman-in-rural-Manitoba-scammed-an-NBA-star-and--322462762.html [https://perma.cc/ADK6-CGT8].

297. Any defamation of Andersen would be examined under the "actual malice"

intentional infliction of emotional distress, and, had he reported the extortion and fake profiles to Facebook and the profiles had been allowed to persist, a violation of Section 230. This would mean that Andersen would have been able to recover damages from Facebook itself, because it would have been liable as a distributor of the damaging content. In the alternative, had Andersen reported the harmful profiles, Facebook would have had a stronger incentive to investigate Chartier's online activities, preventing the false criminal investigation into Andersen before it occurred. While Chartier could still be included as a defendant, adding Facebook to the action would make damage recovery much more likely, and thus the case more attractive and worth the effort and expense to Andersen—and other victims in similar situations who are seeking redress.

Though online impersonation will always be tempting to those who wish to fool others into believing they are someone else, harmful cyber behavior should not be allowed to persist. By amending Section 230 of the Communications Decency Act to narrow website operators' immunity for the harmful content on their sites, important preemptive measures can be taken to prevent dangerous conduct by the entities in the best position to prevent it in the first place, and adequate remedies can be provided for those who are left otherwise unaided.

standard set forth in *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964). *See supra* text accompanying note 292. However, Chartier's behavior in falsely implicating Andersen as a child molester would meet this standard.