Washington and Lee Law Review

Volume 76 | Issue 3 Article 7

Summer 11-7-2019

Reaching Through the "Ghost Doxer:" An Argument for Imposing Secondary Liability on Online Intermediaries

Natalia Homchick
Washington and Lee University School of Law, homchick.n@law.wlu.edu

Reaching Through the "Ghost Doxer:" An Argument for Imposing Secondary Liability on Online Intermediaries

Natalia Homchick*

Table of Contents

* J.D. Candidate, May 2020, Washington and Lee University School of Law; B.A., 2014, University of Notre Dame. Thank you to Professor David Eggert and Professor Christopher Seaman for all their help throughout the Note-writing process. I also want to thank my entire family for their unconditional support of everything I do.

I. Introduction

Imagine you have decided to run for office, to speak out publicly against an injustice, to enter the job market, or even to join a new online forum. Now, imagine after starting your chosen endeavor, you go online to discover that someone who disagrees with your position posted your personal information on the internet and called for others to harass you. To make matters worse, you realize that you cannot determine who posted your personal data.[1] You have been doxed.[2] Because you cannot identify the person who posted your information, where can you turn for recourse? The next logical party is the website where your personal information was posted.[3] Unfortunately, under current laws online intermediaries are typically immunized from liability in these situations.[4] This Note argues that this lack of legal recourse is no longer acceptable in the internet-dominated modern world.

Doxing (or doxxing) is the act of releasing personal information on the internet without consent.[5] The motivations for doxing vary, but this Note focuses on doxing that is done with the intent to cause harm and the need to provide a remedy to the

1. *See infra* notes 79–88 and accompanying text (discussing how one can easily hide their identity online).

2. *See infra* notes 5–13 and accompanying text (explaining doxing in further detail).

3. *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 329 (4th Cir. 1997) (describing how a victim of anonymous cyber-harassment attempted, unsuccessfully, to hold AOL liable).

4. *See infra* Part III (outlining the broad immunity granted to service providers under the Communications Decency Act).

5. *See* Julia M. MacAllister, Note, *The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information*, 85 FORDHAM L. REV. 2451, 2455–56 (2017) (defining doxing). Personal information that is doxed often includes a home address, an email address, a phone number, a social security number, the victim's employer and employer contact information, the victim's family members' contact information, photos of the victim, or photos of the victim's children and where they attend school. *See id.* at 2456 (listing types of personal information).

victim.[6] Doxing originated in the 1990s and quickly gained popularity in the hacking community.[7] Originally, hackers doxed as a revenge tactic against other hackers.[8] A hacker would dox a rival—revealing the rival's identity—to try to open the victim "up to harassment or even law enforcement action."[9] More recently, however, doxing has moved beyond the hacking community and evolved into a form of cyber-harassment.[10]

Doxing is often done anonymously, and it is frequently difficult to identify the perpetrator—the "doxer"—if they wish to hide their identity.[11] Doxers typically post a victim's personal information on social media sites and other websites that are widely available to

---

6. *See* Victoria McIntyre, Note, *Do(x) You Really Want to Hurt Me: Adapting IIED as a Solution to Doxing by Reshaping Intent*, 19 TUL. J. TECH. & INTELL. PROP. 111, 113 (2016) ("The goal of doxing is to scare and intimidate a victim . . . ."); Sameer Hinduja, *Doxing and Cyberbullying*, CYBERBULLYING RES. CTR., https://cyberbullying.org/doxing-and-cyberbullying (last visited Sept. 8, 2019) (stating doxing is done to seek revenge, to bring attention to someone who was previously anonymous, or even just for "kicks") (on file with the Washington and Lee Law Review); *see also* Dylan E. Penza, Note, *The Unstoppable Intrusion: The Unique Effect of Online Harassment and What the United States Can Ascertain from Other Countries' Attempts to Prevent It*, 51 CORNELL INT'L L.J. 297, 304 (2018) (noting doxing is also used as a form of vigilante justice where a doxer will "reveal the information of people in order to punish them for perceived crimes").

7. *See* McIntyre, *supra* note 6, at 114 (explaining the term "dox" is computer hacker shorthand for documents).

8. *See* Mat Honan, *What is Doxing?*, WIRED (Mar. 6, 2014, 1:03 PM), https://www.wired.com/2014/03/doxing/ (last visited Sept. 8, 2019) (describing the origin of doxing as "an old-school revenge tactic that emerged from hacker culture in [the] 1990s") (on file with the Washington and Lee Law Review).

9. *Id*.

10. *See* Nellie Veronika Binder, Note, *From the Message Board to the Front Door: Addressing the Offline Consequences of Race and Gender-Based Doxxing and Swatting*, 51 SUFFOLK U. L. REV. 55, 58 (2018) ("Doxxers now routinely release a person's private information online with the intention of inciting other Internet users to harass that victim."); Nellie Bowles, *How 'Doxxing' Became a Mainstream Tool in the Culture Wars*, N.Y. TIMES (Aug. 30, 2017), https://www.nytimes.com/2017/08/30/technology/doxxing-protests.html (last visited Sept. 8, 2019) (noting doxing originated in the hacking community, but recently "doxxing has emerged from subculture websites like 4Chan and Reddit to become something of a mainstream phenomenon") (on file with the Washington and Lee Law Review).

11. *See* Emma Marshak, *Online Harassment: A Legislative Solution*, 54 HARV. J. ON LEGIS. 503, 505 (2017) ("Half of the victims of online harassment do not know the perpetrators."); *infra* notes 79–85 and accompanying text (outlining how one can mask their identity online).

the public, such as Wikipedia or Twitter.[12] Once someone is doxed, anyone with access to the internet can find and use the information to perpetuate the harassment.[13]

Current examples of doxing are all too common. The home address and phone number of Dr. Christine Blasey Ford, the woman who accused Supreme Court Justice Brett Kavanaugh of sexual assault, were posted on Twitter after she came forward publicly with her accusations.[14] After being doxed, Dr. Ford received death threats and other harassing messages, which ultimately caused her and her family to flee their home.[15] Additionally, during the September 2018 Kavanaugh hearing, three Republican Senators—Lindsey Graham, Mike Lee, and Orrin Hatch—were doxed.[16] The Senators' home addresses and

---

12. *See* Binder, *supra* note 10, at 59–60 ("[B]ecause doxed data remains online until the harasser or the hosting site removes it, the information continues to corrode victims' professional and social reputations long after the initial harassment occurs."); *see, e.g.*, McAllister, *supra* note 5, at 2452 (recounting the doxing of Brianna Wu, who received rape and death threat tweets that included photos of her and her husband and their home address).

13. *See* McIntyre, *supra* note 6, at 112 (noting once personal information is doxed, others can use the information and continue to threaten a victim and often "[i]t is impossible to know who is behind the threats because they are able to hide behind various accounts on the Internet").

14. *See* Jesselyn Cook, *A Troll Doxxed Christine Blasey Ford. Twitter Let Him Back on Its Platform in Hours*, HUFFINGTON POST (Sept. 20, 2018, 12:14 PM), https://www.huffingtonpost.com/entry/troll-doxxed-christine-blasey-ford-twitter_us_5ba3ba6ee4b069d5f9d0ce92 (last visited Sept. 8, 2019) ("[O]thers retweeted the messages and copied them onto Reddit, further disseminating Blasey's contact details.") (on file with the Washington and Lee Law Review).

15. *See id*. (explaining how the rapid dissemination of Dr. Ford's personal information forced her family to flee their home). Brett Kavanaugh's wife, Ashley, received death threats in her government email inbox leading up to the September 2018 hearing. *See* William Cummings & Christal Hayes, *Death Threats Target Brett Kavanaugh's Family, Woman Who Accused Him of Sexual Assault*, USA TODAY (Sept. 20, 2018, 6:35 PM), https://www.usatoday.com/story/news/politics/onpolitics/2018/09/20/death-threats-brett- kavanaugh-christine-blasey-ford/1371995002/ (last visited Sept. 8, 2019) (recounting that Kavanaugh's wife received multiple threatening emails to her government email) (on file with the Washington and Lee Law Review). Because Mrs. Kavanaugh is a Town Manager for the Maryland Village of Chevy Chase, her work email address is available online and her information was not doxed. *See The Village of Chevy Chase Section 5*, VILLAGE OF CHEVY CHASE, http://www.chevychasesection5.org/ (last visited Sept. 8, 2019) (listing Ashley Kavanaugh as Town Manager and providing an email address to contact her) (on file with the Washington and Lee Law Review).

16. *See* Lukas Mikelionis, *Republican Senators Doxxed on Wikipedia by*

personal cell phone numbers were posted on Wikipedia and then shared on Twitter.[17]

Doxing victims also include those not in the public eye. Numerous college professors have been doxed after discussing controversial topics.[18] In Washington state in December 2018, a student secretly filmed his high school teacher's lecture on the Swedish YouTube sensation Felix Kjellberg.[19] During his lecture, the teacher criticized Kjellberg "for promoting racism and anti-Semitism."[20] After the student posted the video on Twitter, followers of Kjellberg made public attempts to gather the teacher's name and personal information to dox him.[21]

Doxing creates harm offline in the real world because the personal information posted is accessible to anyone with an internet connection.[22] Once the personal information is on these public sites, it is available for anyone to view (and use) and difficult to remove.[23] Doxing's harms include harassment, physical harm,

---

Someone from House of Representatives After Kavanaugh Hearing, FOX NEWS (Sept. 28, 2018), https://www.foxnews.com/politics/republican-senators-doxxed-on-wikipedia-by-someone-from-house-of-representatives-after-kavanaugh-hearing (last visited Sept. 8, 2019) ("The leaking of information occurred sometime after the three lawmakers questioned Kavanaugh.") (on file with the Washington and Lee Law Review).

17. *See id*. ("The intentional publication of the information was first caught by a Twitter bot that automatically tracks any changes made to the Wikipedia entries from anyone located in the U.S. Congress and publicizes them on the social media site.").

18. *See* Asia Fields, *Secret Video of Teacher Criticizing YouTuber Goes Viral*, SEATTLE TIMES, Dec. 23, 2018, at B1 ("Some professors have lost jobs or become scared for the safety of their family after being harassed or doxed."); *see also* Bowles, *supra* note 10 (noting a professor from Arkansas who was doxed in 2017 and wrongly accused of participating in a neo-Nazi march).

19. *See* Fields, *supra* note 18, at B1 (discussing that the teacher's lecture on fake news criticized Kjellberg).

20. *Id*.

21. *See id*. (recounting that "Kjellberg saw the post and retweeted it," which led to others also reposting it).

22. *See* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 20 (2014) ("Harassing posts are situated wherever there are individuals who view them and thus they have a profound influence over victims' lives."); Layla Goldnick, Note, *Coddling the Internet: How the CDA Exacerbates the Proliferation of Revenge Porn and Prevents a Meaningful Remedy for Its Victims*, 21 CARDOZO J.L. & GENDER 583, 591 (2015) (articulating how victims of doxing experience real life harms offline when their personal information is posted).

23. *See* Jacqueline D. Lipton, *Combating Cyber-Victimization*, 26 BERKELEY

and financial harm.[24] Doxing victims are also at an increased risk of identity theft.[25]

Doxing tactics also include more severe forms, such as revenge porn[26] or swatting.[27] Revenge porn is the posting of intimate images of another person without permission.[28] The images are typically posted with offensive remarks about the person and often include links to the victim's social media profiles and to other personal information.[29] Swatting is a form of cyber-harassment where someone will call in a false report to authorities that leads police to dispatch heavily armed tactical units to a victim's home.[30] States have criminalized swatting; however, because the call to authorities is typically placed anonymously, the perpetrator often

---

TECH. L.J. 1103, 1112 (2011) (explaining how even if content is removed from one website it can "be cached and copied on other websites"); John B. Major, Note, *Cyberstalking, Twitter, and the Captive Audience: A First Amendment Analysis of 18 U.S.C. § 2261A(2)*, 86 S. CAL. L. REV. 117, 124 (2012) (outlining how even if someone blocks a Twitter user, their posts can still be located in searches).

24. *See* CITRON, *supra* note 22, at 10 (stating that the average cost of cyber-harassment is $1,200 due to legal fees, child care costs, and moving expenses).

25. *See* Marshak, *supra* note 11, at 513 ("Doxxing has an economic impact both when the victim takes expensive preventative measures and when the publication of private information is followed by more harassment or threats."); Binder, *supra* note 10, at 59 (providing that doxing often includes encouragement to cause physical harm to the victim and when a doxer releases social security numbers or other financial account information, doxing raises the victim's potential for identity theft).

26. *See* Goldnick, *supra* note 22, at 585 (discussing revenge porn and explaining how it is becoming more common).

27. *See* Binder, *supra* note 10, at 55 (explaining how swatting and doxing are related).

28. *See* Goldnick, *supra* note 22, at 585–86 (defining revenge porn and discussing the lack of legal recourse for many victims of revenge porn).

29. *See id*. at 586 ("The most damaging revenge websites actually link the illicit content to legitimate social networking and media sites like Facebook, Twitter, and LinkedIn.").

30. *See* Binder, *supra* note 10, at 55 (discussing a Massachusetts Congresswoman who was a swatting victim after an anonymous caller reported the Representative's "home was under attack by an 'active' shooter").

cannot be identified or prosecuted.[31] Existing federal laws do not expressly address swatting.[32]

Swatting often stems from doxing,[33] and it is inherently dangerous because both the SWAT team and the victim are prompted to act based on inaccurate or incomplete information.[34] Swatting has even led to death[35] and the physical injury of victims caught up in these situations.[36] In addition to endangering both police and victims, swatting wastes government resources as first responder teams are deployed to address a non-existent threat.[37]

Doxing can cause harm to anyone who incites the wrath of the cybermob.[38] However, doxing and other forms of cyber-harassment

---

31. *See* CAL. PENAL CODE § 148.3 (West 2014) (criminalizing knowingly making a false report of an emergency); Ryan Grenoble, '*Swatting' is Endangering Lives, Aided in Part by a Legal Loophole*, HUFFINGTON POST (June 7, 2019, 3:59 PM), https://www.huffingtonpost.com/entry/deadly-prank-endangering-lives_us_5b17fca6e4b09578259e132b (last visited Sept. 8, 2019) ("Tracking down and arresting a swatter is often a difficult, costly endeavor, requiring investigators to cross local, state and international borders alike in search of call logs on servers.") (on file with the Washington and Lee Law Review).

32. Grenoble, *supra* note 31.

33. Binder, *supra* note 10, at 55.

34. *See id*. at 60 (explaining why swatting is the most extreme form of doxing); Matthew James Enzweiler, Note, S*watting Political Discourse: A Domestic Terrorism Threat*, 90 NOTRE DAME L. REV. 2001, 2002 (2015) ("The authorities respond with weapons drawn, expecting a high-risk incident, thereby creating a dangerous situation for the unsuspecting swatting victim and police alike.").

35. *See* Brett Molina, *California Man Pleads Guilty After 'Swatting' Call Led to Kansas Man's Death*, USA TODAY (Nov. 14, 2018, 1:40 PM), https://www.usatoday.com/story/news/nation-now/2018/11/14/man-pleads-guilty-call-duty-hoax-leading-deadly-swatting/1999789002/ (last visited Sept. 8, 2019) (describing how a swatting victim was fatally shot by police after a man falsely reported a hostage situation at the victim's home) (on file with the Washington and Lee Law Review).

36. *See* Elizabeth M. Jaffe, *Swatting: The New Cyberbullying Frontier After* Elonis v. United States, 64 DRAKE L. REV. 455, 457, 471 (2016) (recounting the swatting of Tyran Dobbs, who was shot twice with rubber bullets, once in the face, during a swatting incident at his apartment).

37. *See* Binder, *supra* note 10, at 60 (outlining how swatting diverts resources from actual emergencies and wastes taxpayers dollars); Enzweiler, *supra* note 34, at 2003 (noting how swatting is expensive because the false threats mobilize mass responses by authorities).

38. *See* CITRON, *supra* note 22, at 21 ("The United States is not alone in struggling with cyber harassment.").

disproportionately affect women.[39] Women of color encounter more harassment than any other group.[40] Both academic studies and law enforcement studies support this conclusion.[41] On the other hand, men are often attacked online for their ideas or actions.[42] In short, doxing causes real harm and society is slowly starting to recognize the true cost of this behavior.

Despite growing awareness of doxing's pernicious consequences, existing laws do not adequately address either the underlying behavior or its consequences.[43] Some signs of progress, however, are emerging. Proposed legislation in the U.S. House of Representatives—the Online Safety Modernization Act of 2017 (Online Safety Act)[44]—would provide for federal criminal and civil liability for doxing.[45] This bill is a step forward, but it does not address the lack of legal recourse for a victim if the person posting the information cannot be identified.[46] This Note aims to explain

---

39. *See id.* at 13 ("Of the 3,393 individuals reporting cyber harassment to WHOA [Working to Halt Online Abuse] from 2000 to 2011, 72.5 percent were female and 22.5 percent were male (5 percent were unknown)."); Binder, *supra* note 10, at 61 ("Online harassers routinely objectify women on their physical appearances, and doxxing is regularly accompanied by threats of sexual violence.").

40. *See* CITRON, *supra* note 22, at 14 ("Nonwhite females face cyber harassment more than any other group, with 53 percent reporting having been harassed online.").

41. *See id.* ("The most recent Bureau of Justice Statistics report found that seventy-four percent of individuals who were stalked on- or offline were female, and twenty-six percent were male."); Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 373 (2009) ("Grappling with the trivialization of cyber gender harassment is a crucial step to understanding and combating the harm that it inflicts.").

42. *See* CITRON, *supra* note 22, at 15 ("When men face cyber harassment, their experience often resonates with the abuse faced by women.").

43. *See* Binder, *supra* note 10, at 56 (explaining current laws do not adequately address doxing or swatting); Lipton, *supra* note 23, at 1106 ("The prevalence of this conduct suggests that more effective means are necessary to redress online wrongs and to protect victims' reputations, but action against cyber-abusers has posed significant challenges for the legal system.").

44. H.R. 3067, 115th Cong. (2d Sess. 2017).

45. *See id.* (proposing to amend the federal criminal code for doxing and swatting).

46. *See* Binder, *supra* note 10, at 63 ("Harassers can post destructive content anonymously, and often evade law enforcement officials by exploiting location-obstructing technology and jurisdictional boundaries.").

why it is appropriate, and necessary, to hold online intermediaries secondarily liable when the doxer cannot be identified.

For the purposes of this Note, an online intermediary is a company that facilitates access to the internet.[47] The phrase is broad and encompasses internet service providers, search engines, and social media platforms.[48] Throughout this Note, the unidentified doxer will be referred to as the "ghost doxer" and the target of the doxing will be referred to as the "victim."

This Note contends in Parts II–III that the standards of conduct to which the public holds online intermediaries have changed since the internet developed in the early 1990s. As a result, the Communications Decency Act of 1996 (CDA)[49]—which offers broad immunity to online intermediaries for content posted by third-parties—should be amended to address the harm caused by doxing. The doxing CDA amendment could parallel the 2018 sex-trafficking CDA amendment and allow an online intermediary to be potentially liable if violations of the new federal law on doxing and ghost doxing occur on their site.[50]

Part IV argues that copyright law can provide a model for legislation to impose secondary liability on online intermediaries for ghost doxing. Under copyright law, secondary liability is broken into two categories—contributory liability and vicarious liability.[51] Therefore, the ghost doxing liability scheme could have two components. First, online intermediaries that encourage doxing could be held liable under a contributory liability theory.[52] Under

---

47. *See* KARINE PERSET, THE ECONOMIC AND SOCIAL ROLE OF INTERNET INTERMEDIARIES 9 (2010) (stating internet intermediaries "facilitate transactions between third parties on the internet"), https://www.oecd.org/internet/ieconomy/44949023.pdf.

48. *Frequently Asked Questions on Internet Intermediary Liability*, ASS'N FOR PROGRESSIVE COMMS., https://www.apc.org/en/pubs/apc%E2%80%99s-frequently-asked-questions-internet-intermed (last visited Sept. 8, 2019) (listing types of internet intermediaries such as network operators, internet access providers, internet service providers, hosting providers, search engines, social networks, and other blogs or websites with comment sections) (on file with the Washington and Lee Law Review).

49. Communications Decency Act of 1996, 47 U.S.C. § 230 (2012).

50. *See infra* Part III.B (delineating this Note's proposed doxing § 230 amendment).

51. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 434–35 (1984) (discussing copyright law's secondary liability scheme).

52. *See infra* Part IV (outlining copyright's secondary liability scheme and

copyright law, contributory copyright infringement occurs when one intentionally induces or encourages direct infringement.[53] Second, for websites where non-inducement doxing occurs, online intermediaries could be held vicariously liable in instances where notice is given and the online intermediary fails to remove the doxing content.[54] Vicarious liability in copyright can be imposed when one has "the right and ability to supervise the infringing activity and also has a direct financial interest in such activities."[55] This Note argues the doxing notice and takedown provision could be modeled off the Digital Millennium Copyright Act (DMCA),[56] which provides safe harbor provisions for internet service providers who remove copyright infringing material following written notice.[57] Overall, this Note proposes a ghost doxing liability scheme—modeled off copyright law's secondary liability theories—be added into the proposed federal bill on doxing.

II. Times Have Changed for Online Intermediaries

The internet is no longer a new frontier that should be afforded Wild West status.[58] New laws are needed because today's internet is far more pervasive and has a completely different configuration than the internet when it was first developed.[59] First, the number

---

arguing how it can be applied to doxing).

53. *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005) (describing contributory copyright infringement).

54. *See infra* Part IV (explaining how copyright law's secondary liability scheme can be applied to doxing).

55. Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971) (citations omitted).

56. 17 U.S.C. §§ 512, 1201–1205, 1301–1332, 28 U.S.C. § 4001 (2012).

57. *See* 17 U.S.C. § 512 (providing various safe harbors from indirect copyright infringement for internet service providers who comply with the statute).

58. *See* CITRON, *supra* note 22, at 79, 102 (arguing the notion of the Wild West internet is "based on a false set of assumptions").

59. *See id*. at 102 ("Just as harm in the workplace and home have profound social consequences, so too does harassment in networked spaces."); Marshak, *supra* note 11, at 504 ("Online threats and harassment are a growing problem as life moves online, and the current set of state laws, which were mostly developed in the 1990s, generally lack the vocabulary and framework to address criminal behavior that occurs in cyberspace rather than physical space.").

of people with consistent internet access in the 1990s was a fraction of what it is now.[60] Second, blogs and other online discussion boards—which are the epicenter of cyber-harassment—did not even exist in the mid-1990s.[61] Third, many of the behemoth online companies that currently dominate the online marketplace, such as Facebook, did not exist in the 1990s.[62]

Today, more than one billion people use Facebook daily.[63] The reach and influence of companies such as Facebook was unimaginable in the mid-1990s.[64] Congress is just beginning to discuss the need to address the issues created by the reach of these companies.[65] The April 2018 congressional hearing with Facebook's CEO Mark Zuckerberg supports the contention that the standard to which the public holds online intermediaries is tightening.[66] During the hearing, Senator Chuck Grassley stated, "[t]he tech industry has an obligation to respond to widespread and growing concerns over data privacy and security and to restore the

---

60. *See* Reuben Fischer-Baum, *What 'Tech World' Did You Grow Up In?*, WASH. POST (Nov. 26, 2017), https://perma.cc/MCV5-EKZF (last visited Sept. 8, 2019) (noting that in 1996 seventy-five percent of American households had no internet) (on file with the Washington and Lee Law Review).

61. *See* Ann Bartow, *Internet Defamation as Profit Center: The Monetization of Online Harassment*, 32 HARV. J.L. & GENDER 383, 390 (2009) ("[T]he Internet was structured very differently in 1996, and the opportunities for anonymous harassment of women outside of community structures were far fewer, as blogs and online discussion boards as currently structured did not exist.").

62. *See Facebook*, FACEBOOK, https://www.facebook.com/pg/facebook/about/?ref=page_internal (last visited Sept. 8, 2019) (stating Facebook was founded on February 4, 2004) (on file with the Washington and Lee Law Review).

63. *See Facebook, Social Media Privacy, and the Use and Abuse of Data*: *Hearing Before the U.S. S. Comm. on the Judiciary and the U.S. S. Comm. on Commerce, Sci., and Transp.*, 115th Cong. (2018) (statement of Senator John Thune) [hereinafter *Facebook Comm. Hearing*] ("More than 2 billion people use Facebook every month 1.4 billion people use it every day; more than the population of any country on Earth except China, and more than four times the population of the United States."),http://www.astrid-online.it/static/upload/zuck/zuckerberg_senate-hearing-transcript_10_04_18.pdf.

64. *Id*.

65. *See id*. (statement of Senator Bill Nelson) ("And, if Facebook and other online companies will not or cannot fix the privacy invasions, then we are going to have to—we, the Congress.").

66. *See id*. (statement of Senator John Thune) ("We want to hear more, without delay, about what Facebook and other companies plan to do to take greater responsibility for what happens on their platforms.").

public's trust. The status quo no longer works."[67] These hearings are strong evidence that society is starting to demand that online intermediaries be held to a higher standard than they were in the early days of the internet.[68]

A. Proposed Federal Doxing Legislation—Online Safety Modernization Act of 2017

Members of Congress are starting to recognize the need to address cyber-harassment (such as doxing) through specific legislation.[69] The proposed Online Safety Act bill addresses both criminal and civil liability.[70] Doxing would be a criminal violation: Whoever uses the mail or any facility or means of interstate or foreign commerce, to *knowingly publish a person's personally identifiable information*—(1) with the *intent to threaten, intimidate, or harass any person,* incite or facilitate the commission of a crime of violence against any person, or place any person in reasonable fear of death or serious bodily injury; or (2) with the *intent that the information will be used to threaten, intimidate, or harass any person*, incite or facilitate the commission of a crime of violence against any person, or place any person in reasonable fear of death or serious bodily injury, shall be fined under this title or imprisoned not more than 5 years, or both.[71]

---

67. *Id.* (statement of Senator Chuck Grassley).

68. *See id*. (statement of Senator John Thune) ("In the past, many of my colleagues on both sides of the aisle have been willing to defer to tech companies' efforts to regulate themselves, but this may be changing."); *see also* Jaffe, *supra* note 36, at 467 (discussing how "the reasonable standard may change in favor of the broadcaster to cast a wider security net over the channels being used").

69. *See* H.R. 3067, 115th Cong. (2d Sess. 2017) (listing the sponsor of the proposed federal doxing bill as Representative Katherine Clark from Massachusetts and indicating co-sponsors, including representatives from Indiana, California, Florida, Georgia, New Hampshire, Pennsylvania, and Tennessee).

70. *See id*. (proposing the section "Interstate Doxxing Prevention" which would amend 18 U.S.C. §§ 871-880 to hold a doxer criminally liable and provide a civil cause of action to a victim).

71. *Id*. (emphasis added).

Further, Title II of the bill proposes criminal and civil liability for swatting.[72] The bill also directs the Department of Justice to develop a strategy to reduce, investigate, and prosecute cybercrimes against individuals, and to publish statistics on cybercrimes against individuals.[73]

Massachusetts Representative Katherine Clark, the sponsor of the Online Safety Act, is one of Congress's most avid anti-doxing advocates.[74] The Congresswoman was even a swatting victim herself in 2016.[75] Representative Clark has introduced multiple bills that address swatting and other forms of cyber-harassment.[76] Unfortunately, none of these proposed bills have been passed into law.[77] On the whole, these proposed bills on doxing and swatting acknowledge the growing need for doxing victims to have legal recourse. The various proposed doxing bills, however, do not address individuals victimized by ghost doxers.[78]

B. Anonymity on the Internet

The problem of the ghost doxer is common and should not be ignored.[79] Today, anonymity on the internet can be achieved with

---

72. *See id*. (proposing criminal liability for anyone who "knowingly transmit[s] false or misleading information that would reasonably be expected to cause an emergency response" in the absence of circumstances reasonably requiring an emergency response).

73. *See id.* ("The Attorney General shall develop a national strategy to reduce the incidence of cybercrimes against individuals . . . .").

74. *See* Lisa Bei Li, Note, *Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting*, 70 FED. COMM. L.J. 317, 325 (2018) (discussing Representative Clark's various anti-doxing proposals).

75. *See* Press Release, Katherine Clark, U.S. Representative for the 5th District of Massachusetts, Congresswoman Katherine Clark Target of Swatting Hoax (Feb. 3, 2016) (explaining on the evening of January 31, 2016 the police received an anonymous call claiming there was an active shooter at Representative Clark's home) (on file with the Washington and Lee Law Review).

76. *See* Li, *supra* note 74, at 325 (stating Representative Clark sponsored multiple bills to combat cyber-harassment).

77. *See id*. (noting none of the proposed bills on doxing or swatting have been enacted by Congress yet).

78. *See* CITRON, *supra* note 22, at 221–24 (indicating that online harassers cannot be prosecuted if the individual cannot be identified).

79. *See* Lipton, *supra* note 23, at 1114 ("The anonymity provided by the Internet may increase the volume of abusive conduct because it may encourage individuals who would not engage in such conduct offline to do so in the

relative ease.[80] For example, Tor is an internet network that allows its users to remain anonymous online by hiding their IP addresses.[81] To make matters worse, ghost doxers are more likely to be bolder and tend to go further than when their identity is known.[82] While in some instances a victim can obtain a court order to identify a ghost doxer, these "John Doe" subpoenas are often difficult to obtain.[83] A court will issue a John Doe subpoena only after the victim navigates the procedural requirements and makes the necessary showing required by the authorizing law or rule.[84]

---

anonymous virtual forum provided by the Internet—people are less inhibited when faced with a computer terminal . . . ."); Marshak, *supra* note 11, at 523 (proposing legislation on doxing and noting "that even anonymous communication is criminalized [in the proposed legislation] so that future developments in related laws, such as those governing the statute of protective orders, will be easily transferred to this statute"); Binder, *supra* note 10, at 63 (noting harassers often post anonymously and use technology to avoid being identified).

80. *See* Miriam R. Albert, *E-Buyer Beware: Why Online Auction Fraud Should Be Regulated*, 39 AM. BUS. L.J. 575, 592 n.74 (2002) (explaining that one's online identity can be concealed through the use of "anonymous emails, short-lived Web-sites, and falsified domain name registrations"); Michael Froomkin, *"PETs Must Be on a Leash": How U.S. Law (and Industry Practice) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology*, 74 OHIO ST. L.J. 965, 986 (2013) (discussing how Internet Protocol (IP) numbers can be masked to conceal one's identity); Kristine Gallardo, Note, *Taming the Internet Pitchfork Mob: Online Public Shaming, the Viral Media Age, and the Communications Decency Act*, 19 VAND. J. ENT. & TECH. L. 721, 729 (2017) ("[T]he existence of an IP address alone, without additional identifying information, cannot pinpoint the absolute identity of an online poster.").

81. *See* McIntyre, *supra* note 6, at 114 ("Doxbin, a Tor site used to host files containing the personal information of individuals and certain groups of people, was launched in 2011."); *Tor FAQ*, TOR PROJECT, https://www.torproject.org/docs/faq.html.en#WhatIsTor (last visited Sept. 8, 2019) ("Tor is a program you can run on your computer . . . [i]t protects you by bouncing your communications around a distributed network of relays . . . it prevents somebody watching your Internet connection from learning what sites you visit . . . .") (on file with the Washington and Lee Law Review).

82. *See* Nancy S. Kim, *Web Site Proprietorship and Online Harassment*, 2009 UTAH L. REV. 993, 1009 [hereinafter *Web Site Proprietorship*] ("Anonymity also reduces accountability and accuracy."); Gallardo, *supra* note 80, at 728 ("[I]t is much easier to criticize someone's actions when you can do so anonymously.").

83. *See* CITRON, *supra* note 22, at 223 ("Courts protect the identity of anonymous posts from frivolous lawsuits by setting forth a series of requirements before granting these [John Doe] subpoenas.").

84. *See* Nathaniel Gleicher, Note, *John Doe Subpoenas: Toward a Consistent Legal Standard,* 118 YALE L.J. 320, 325 (2008) (noting how the standard courts use for John Doe subpoenas is varied).

Overall, it is relatively easy for a doxer to shield their identity online if they have a desire to do so.[85] Anonymity online, however, has many benefits.[86] For example, anonymity online can allow those dealing with sensitive issues—such as domestic violence survivors seeking support—to receive assistance that they otherwise might not obtain.[87] Therefore, this Note does not argue that anonymity online should be discouraged or that anonymous online speech is detrimental. Rather, this Note argues that the laws surrounding the discourse on the internet must be updated to reflect the modern reality of cyber-crimes and cyber-harassment such as doxing.[88]

C. Privacy and First Amendment Concerns with Regulating Doxing

Doxing inherently implicates both an individual's privacy and free speech.[89] Free speech advocates sometimes express concern about regulating cyber-harassment because of the potential chilling effect on free speech.[90] A full discussion of the potential

---

85. *See* CITRON, *supra* note 22, at 55 (recounting a blogger experiencing cyber-harassment who was unable to identify her harassers even with the assistance of a paid forensic computer expert); Binder, *supra* note 10, at 71 ("Moreover, the anonymity of the web makes it difficult for victims to know who is attacking them, and the lack of legal repercussions for unmasked harassers has only emboldened doxxers and swatters."); Russell Brandom, *Finding Fuboy: One Man Spent Four Years and $35,000 to Unmask His Internet Troll*, VERGE (Nov. 23, 2018, 8:50 AM), https://www.theverge.com/2015/11/23/9772824/commenter-defamation-lawsuit-identity-revealed (last visited Sept. 8, 2019) (examining the story of a politician in Illinois who sought to identify the person who had compared him to Jerry Sandusky online) (on file with the Washington and Lee Law Review).

86. *See* CITRON, *supra* note 22, at 60–61 (explaining anonymity online has many benefits, such as support for marginalized groups).

87. *Id*.

88. *See id*. at 20 (stating cyber-harassment is a major issue that needs to be addressed).

89. *See id*. at 190 (arguing a legal regime governing cyber-harassment would not necessarily "undermine our commitment to free speech"); MacAllister, *supra* note 5, at 2462 (noting how as technology evolves notions of privacy also evolve).

90. *See* CITRON, *supra* note 22, at 191 ("Many resist the regulation of the online speech as antithetical to our commitment to public discourse because the Internet is the 'equivalent of the public square.'"); Lipton, *supra* note 23, at 1128 (discussing how the First Amendment is implicated when attempting to regulate

First Amendment challenges to doxing legislation is outside the scope of this Note. However, it is important to momentarily discuss the competing doctrines of privacy and free speech because speech on the internet can have a global reach almost instantly and a lasting effect.[91]

Justice Louis Brandeis stated that "the right to be let alone [is] the most comprehensive of rights and the right most valued by civilized men."[92] Privacy consists of two main constitutional values: "the individual interest in avoiding disclosure of personal matters" and "the interest in independence in making certain kinds of important decisions."[93] Doxing uniquely implicates both of these values, as many times the doxed content will follow the victim online for an extended period of time.[94] Privacy interests, however, must be balanced by free speech considerations.[95]

The First Amendment provides that "Congress shall make no law . . . abridging the freedom of speech."[96] First Amendment jurisprudence rests on the idea that "the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable."[97] The Supreme Court articulated in *Reno v. American Civil Liberties Union*[98] that online speech is awarded the same First Amendment protection as offline speech.[99] The right to free speech, however, is not absolute and some categories of speech are not protected.[100]

---

cyber-harassment).

91. *See* Gallardo, *supra* note 80, at 728 (stating an estimated 3.2 billion people have access to the internet).

92. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

93. U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 762 (1989) (quoting Whalen v. Roe, 429 U.S. 589, 589–600 (1977)).

94. *See* MacAllister, *supra* note 5, at 2462 (explaining how online content can often remain viewable for a long time).

95. *See id.* ("The right to privacy is not absolute . . . .").

96. U.S. CONST. amend. I.

97. Texas v. Johnson, 491 U.S. 397, 414 (1989).

98. 521 U.S. 844 (1997).

99. *See id.* at 870 (discussing the internet, the Supreme Court stated "[w]e agree . . . that our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium").

100. *See* Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942) ("These include the lewd and obscene, the profane, the libelous, and the insulting or 'fighting' words—those which by their very utterance inflict injury or tend to

Regulating doxing illuminates the tension between privacy and free speech. In *Cohen v. California*,[101] the Supreme Court stated the ability to regulate speech depends on whether "substantial privacy interests are being invaded in an essentially intolerable manner."[102] Doxing is arguably invading a substantial individual privacy interest in an intolerable manner because of the harm doxing causes offline.[103]

Further, conduct, unlike speech, is not under First Amendment protection.[104] Focusing on the conduct aspect could reduce or avoid First Amendment concerns for doxing.[105] Overall, attempts to regulate online speech will likely be met with First Amendment challenges.[106] Congress (hopefully) can draft a statute for doxing that mitigates potential First Amendment challenges.[107]

III. Amending the Communications Decency Act for Doxing

Congress's careful drafting of a federal law on doxing should be done in conjunction with an amendment to the Communications

---

incite an immediate breach of the peace."). Threats are also not constitutionally protected. *See* Virginia v. Black, 538 U.S. 343, 358–59 (2003) (explaining the First Amendment permits Congress or a state to ban a "true threat"); *see also* Watts v. United States, 394 U.S. 705, 708 (1969) (stating political hyperbole is not a true threat).

101. 403 U.S. 15 (1971).

102. *Id*. at 21.

103. *See supra* notes 22–42 and accompanying text (describing the offline harm doxing causes).

104. *See* United States v. O'Brien, 391 U.S. 367, 376 (1996) ("We cannot accept the view that an apparently limitless variety of conduct can be labeled 'speech' whenever the person engaging in the conduct intends thereby to express an idea."); *Cohen*, 403 U.S. at 27 (Blackmun, J., dissenting) ("Cohen's absurd and immature antic, in my view, was mainly conduct and little speech.").

105. *See* Li, *supra* note 74, at 320 (arguing the best way to mitigate First Amendment issues with regulating doxing and swatting is to focus on the conduct aspect of both).

106. *See* MacAllister, *supra* note 5, at 2463 (explaining likely First Amendment challenges to doxing will be that the statute is void for vagueness and overly broad).

107. *Cf.* Lipton, *supra* note 23, at 1128 ("In the physical world, statutes have successfully criminalized offline analogs to many of today's online wrongs. There is no reason why judges cannot continue to draw lines between protected and prohibited speech in the online context.").

Decency Act (CDA) of 1996.[108] The CDA, also referred to as § 230, was originally enacted when the internet was still in its infancy to allow for the development of the new medium.[109] Specifically, the CDA was enacted in part as a response to *Stratton Oakmont, Inc. v. Prodigy Services Co.*[110] *Stratton Oakmont* was a New York state court case that found Prodigy, a computer network with two million subscribers, liable for an anonymous defamatory message posted on one of its online bulletin boards—"Money Talk."[111] The court found that Prodigy was a publisher—and subject to defamation liability—because it filtered some offensive content from its site.[112]

Under the reasoning of *Stratton Oakmont*, interactive computer services could escape liability if they never removed offensive content, but they would be subject to liability if they ever removed offensive content.[113] In enacting the CDA, "Congress sought to immunize the *removal* of user-generated content, not the *creation* of content" and thus avoid penalizing online intermediaries for removing offensive material.[114] Further, the CDA is particularly powerful because it preempts any state or local laws that are inconsistent with it.[115] Specifically,

---

108. 47 U.S.C. § 230.

109. *See id.* § 230(a) (noting the Congressional finding that "[t]he Internet and other interactive computer services have flourished to the benefit of all Americans, with a minimum of government regulation").

110. No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995); *see* Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997) (discussing how Congress passed CDA § 230 in part as a response to *Stratton Oakmont* and aimed to encourage interactive computer services to "self-regulate the dissemination of offensive material over their services"); Goldnick, *supra* note 22, at 599 (explaining Congress passed CDA in response to *Stratton Oakmont*).

111. *See Stratton Oakmont*, 1995 WL 323710, at *1–2 (describing how the defendant's website functioned).

112. *See id.* at *10 ("[T]his Court is compelled to conclude that for the purposes of plaintiff's' claims in this action, Prodigy is a publisher . . . .").

113. *Cf.* Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1163 (9th Cir. 2008) (discussing how Congress in passing the CDA sought to overturn *Stratton Oakmont*).

114. *Id.*

115. *See* § 230(e)(3) ("No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."); Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1105 (9th Cir. 2009) (holding Yahoo! was immune from liability under CDA § 230(c)(1) for an Oregon state law negligent undertaking claim when the company did not remove the offensive content

§ 230(c)—Protection for "Good Samaritan" Blocking and Screening of Offensive Material—states "[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."[116] Thus, an online intermediary enjoys immunity unless it crosses the line from service provider to content provider.[117]

A. Lessons from Zeran v. American Online *and* Barnes v. Yahoo!

Zeran v. America Online, Inc.[118]—an early ghost doxing case[119]—was instrumental in extending broad § 230 immunity to internet service providers.[120] The plaintiff Ken Zeran was wrongly associated with many offensive anonymous posts about the Oklahoma City Bombing.[121] The anonymous posts, which began within a week of the bombing, advertised the sale of shirts and other merchandise "featuring offensive and tasteless slogans related to the bombing."[122] The advertisements included Zeran's home phone number and instructed viewers to call Zeran regarding the merchandise.[123] The anonymous poster continued to advertise additional merchandise online, and "interested buyers

---

Barnes' former boyfriend posted on their site); *see also* Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 672 (8th Cir. 2008) ("[G]iven § 230(c)(1) it cannot sue the messenger just because the messenger reveals a third party's plan to engage in unlawful discrimination.").

116. 47 U.S.C. § 230(c).

117. *See Barnes*, 570 F.3d at 1100–01 ("[S]ubsection (c)(1) only protects from liability (1) a provider or user of an interactive computer services (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider."); Goldnick, *supra* note 22, at 601–02 (articulating the difference between an internet service provider and an online content provider).

118. 129 F.3d 327 (4th Cir. 1997), *cert. denied*, 524 U.S. 937 (1998).

119. *See id*. at 329 (outlining that the plaintiff's claim against AOL was based on a series of anonymous postings).

120. *See* Bartow, *supra* note 61, at 390 (stating *Zeran* was the instrumental case in establishing internet service provider (ISP) immunity under § 230).

121. *See Zeran*, 129 F.3d at 329 (providing that the Oklahoma City Bombing took place on April 19, 1995).

122. *Id*.

123. *See id*. (explaining Zeran could not change his home phone number because he ran his business out of his house).

were told to call Zeran's phone number."[124] Due to these posts, Zeran received numerous angry and threatening calls, including death threats.[125] Zeran contacted AOL and requested that they remove the posts.[126] Ultimately, Zeran sued AOL for the defamatory speech on its platform posted by an unknown third party.[127] The Fourth Circuit found that AOL fit squarely within § 230 and was therefore immune.[128] Zeran had no other recourse as he could not identify his ghost doxer.[129]

Additionally, one of the most concerning aspects of § 230 is that online intermediaries continue to enjoy immunity even after a victim notifies them of doxed content and requests its removal.[130] *Barnes v. Yahoo!, Inc.*[131] provides a striking example. In 2004, Cecilia Barnes ended a relationship with her boyfriend.[132] He responded by posting nude photos of Barnes on various Yahoo! profiles without her permission.[133] The profiles also "included the addresses, real and electronic, and the telephone number at Barnes' place of employment."[134] Barnes's ex-boyfriend also posted in online chat rooms and directed male correspondents to the

---

124. *Id*.

125. *See id*. ("By April 30, Zeran was receiving an abusive phone call approximately every two minutes.").

126. *See id*. ("The parties dispute the date that AOL removed this original posting from its bulletin board.").

127. *See id*. at 330 (noting that AOL raised § 230 as an affirmative defense).

128. *See id*. at 332 ("AOL falls squarely within this traditional definition of a publisher and, therefore is clearly protected by § 230's immunity.").

129. *See id*. at 329 n.1 (quoting Zeran's statement that AOL "made it impossible to identify the original party by failing to maintain adequate records of its users"); DAVID J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 152 (2007) ("He couldn't track down the anonymous person who posted the T-shirt ads. He couldn't sue AOL. He had no way to fight back.").

130. *See* Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1105–06 (9th Cir. 2009) (granting § 230 immunity to Yahoo! even following requests to take down the specific fraudulent profiles of the plaintiff); Zeran v. Am. Online, Inc., 129 F.3d 327, 329 (4th Cir. 1997) (detailing that the plaintiff notified AOL of the defamatory content).

131. 570 F.3d 1096 (9th Cir. 2009).

132. *See id*. at 1098 (explaining the doxing of Barnes).

133. *See id*. (discussing that Barnes did not know the nude photographs of her had been taken).

134. *Id*.

profiles he created.[135] Shortly following this, Barnes began to receive unsolicited emails, phone calls, and visits from men—all with the expectation of sex.[136] Barnes contacted Yahoo! and asked the site to remove the profiles, but the company failed to take any action.[137] Yahoo! eventually promised they would take the profiles offline, but never actually acted until after Barnes filed suit in Oregon state court.[138] The Ninth Circuit affirmed the lower court's ruling that § 230 immunized Yahoo! despite the company's awareness of the profiles.[139] Online intermediaries should not continue to be permitted to hide behind § 230's broad immunity today if they are made aware of specific doxing content.[140]

B. Why the CDA's Broad Immunity is No Longer Appropriate

In addition to stories such as Cecilia Barnes and Ken Zeran, there are a number of reasons why the CDA should be amended to permit lawsuits against online intermediaries. First, one of the main rationales for the CDA, the self-regulation of the internet, has not played out in practice.[141] Second, Congress amended § 230

---

135. *See id.* (describing how Barnes' ex-boyfriend continued to post to draw attention to the profiles he created).

136. *See id.* (stating numerous men sent Barnes unsolicited messages indicating they expected to have sexual relations with her).

137. *See id.* ("One month later, Yahoo! had not responded but the undesired advances from unknown men continued; Barnes again asked Yahoo! by mail to remove the profiles.").

138. *See id.* at 1099 (noting Barnes filed suit after approximately two months of not hearing from Yahoo!).

139. *See id.* at 1105 ("To summarize, we hold that section 230(c) bars Barnes' claim, under Oregon law, for negligent provision of services that Yahoo undertook to provide."). It should be noted that the Ninth Circuit found Yahoo! could potentially be liable under the contract theory of promissory estoppel. *Id.* at 1109. The court ruled that Barnes could have potentially a breach of contract claim based on an estoppel theory because Yahoo! promised to remove the profiles and Barnes had relied on that promise. *Id.* The Ninth Circuit, however, did not rule on the existence of a contract regarding this claim. *Id.*

140. *See infra* Part III.B (explaining why and how the CDA should be amended for doxing).

141. *See* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1122 (9th Cir. 2003) (stating Congress enacted the CDA "to promote the free exchange of information and ideas of the internet and to encourage monitoring for offensive or obscene material").

last year to limit the immunity of websites that facilitate sex trafficking.[142] Third, a growing number of commentators have proposed amending § 230 for various types of cyber-harassment due to the evolution and growth of the internet since 1996.[143]

First, the self-regulation of the internet has not played out in practice as Congress envisioned in 1996.[144] Websites that

---

142. *See* 47 U.S.C. § 230(e)(5) (2012) (providing "[n]othing in this section, other than subsection (c)(2)(A) shall be construed to impair or limit" sex trafficking law); H.R. REP. NO. 115-572(l), at 3 (2018) (explaining the amendment is "designed to combat online sex trafficking by providing new tools to law enforcement . . . by making it easier for states to prosecute criminal actor websites by amending section 230 of the Communications Decency Act"); *Facebook Comm. Hearing*, *supra* note 63 (statement of Senator John Thune) (noting how Congress passed the sex trafficking amendment "in overwhelming bipartisan fashion"); Jeffrey Neuburger, *FOSTA Signed into Law, Amends CDA Section 230 to Allow Enforcement Against Online Providers for Knowingly Facilitating Sex Trafficking*, PROSKAUER, https://newmedialaw.proskauer.com/2018/04/11/fosta-signed-into-law-amends-cda-section-230-to-allow-enforcement-against-online-providers-for-knowingly-facilitating-sex-trafficking/ (last visited Sept. 8, 2019) [hereinafter *FOSTA Signed into Law*] (discussing how the FOSTA amendment aims to encourage online providers to "exercise greater responsibility over sex-trafficking related content") (on file with the Washington and Lee Law Review).

143. *See* CITRON, *supra* note 22, at 177–81 (proposing an amendment to limit immunity under § 230 to exclude "[web]sites that encourage cyberstalking or nonconsensual pornography and make money from its removal *or* that principally host cyber stalking or nonconsensual pornography"); Derek Bambauer, *Exposed*, 98 MINN. L. REV. 2025, 2028–29 (2014) (outlining various scholars' proposed amendments to CDA § 230 to limit the immunity granted to online intermediaries); Nancy S. Kim, *Website Design and Liability*, 52 JURIMETRICS J. 383, 383 (2012) [hereinafter *Website Design and Liability*] (arguing for amending § 230, but creating safe harbors for "website operators that: (1) permit only postings by identified posters; (2) have nonprofit status and do not accept ad revenue; and (3) remove postings upon request of the victim"); Goldnick, *supra* note 22, at 602–04, 626 (explaining various scholarly proposals for amending CDA § 230 and arguing the CDA should be amended for websites that "encourage the posting of illegal or tortious content or contribute materially to illegal or tortious conduct are not afforded immunity"); *see also Web Site Proprietorship*, *supra* note 82, at 999, 1034 (arguing imposing proprietorship liability on web site sponsors through anti-cyber-harassment policy "is consistent with section 230, as it holds the Web site sponsor accountable for its own actions or omissions"); s*ee generally* Matthew G. Jeweler, Note, *The Communications Decency Act of 1996: Why § 230 is Outdated and Publisher Liability for Defamation Should Be Reinstated Against Internet Service Providers*, 8 PITT. J. TECH. L. & POL'Y 1 (2008).

144. *See* CITRON, *supra* note 22, at 171 ("Courts have roundly immunized site operators from liability even though they knew or should have known that user-generated content contained defamation, privacy invasions, intentional inflictions of emotional distress, and civil rights violations.").

knowingly host cyber stalking or revenge porn are likely protected under § 230 and are far from the "Good Samaritans" Congress meant to protect when it drafted the CDA.[145] Further, many websites (such as Twitter) technically have policies that prohibit doxing.[146] Twitter, however, is notorious for not enforcing its own policies.[147] The ideal of internet self-regulation is not the current reality.[148] The actual reality necessitates a change in the existing internet regulatory scheme.[149]

Second, Congress already recognized the need to update the CDA by passing its 2018 amendment to limit immunity for sites that facilitate sex trafficking.[150] The amendment limits the immunity provided by § 230 "for online services that knowingly host third-party content that promotes or facilitates sex trafficking."[151] While this amendment is narrow, Congress's willingness to amend the CDA demonstrates the heightened

---

145. *See id*. at 173 ("Courts have repeatedly found that generalized knowledge of criminal activity on a site does not suffice to transform a site operator into a co-developer or co-creator of the illegal content.").

146. *See About Private Information on Twitter*, TWITTER, https://help.twitter.com/en/rules-and-policies/personal-information (last visited Sept. 8, 2019) ("Twitter Rules: You may not publish or post other people's private information without their express authorization and permission.") (on file with the Washington and Lee Law Review).

147. *See* Cook, *supra* note 14 (articulating Twitter is "notoriously bad at addressing" issues such as doxing even though such practices are against its policies).

148. *See Facebook Comm. Hearing*, *supra* note 63 (statement of Senator John Thune) ("In the past, many of my colleagues on both sides of the aisle have been willing to defer to tech companies' efforts to regulate themselves, but this may be changing.").

149. *See, e.g.*, CITRON, *supra* note 22, at 177 (stating the CDA should be amended for "sites that encourage cyber stalking or non-consensual pornography and make money from its removal *or* that principally host cyber talking or nonconsensual pornography"); *but see* Gallardo, *supra* note 80, at 721 (arguing the CDA empowers web hosts to implement policies that can help curb online public shaming).

150. *See* H.R. REP. NO. 115-572(l), at 3 (2018) (explaining the amendment is "designed to combat online sex trafficking by providing new tools to law enforcement . . . by making it easier for states to prosecute criminal actor websites").

151. *See FOSTA Signed into Law*, *supra* note 142 (describing how the amendment encourages online providers to "exercise greater responsibility over sex-trafficking related content").

standards for online intermediaries in today's internet environment.[152]

Third, numerous commentators have urged Congress to amend the CDA to address the growing problem of cyber-harassment.[153] Further, some have suggested the DMCA's takedown notice provisions could provide a model for a § 230 amendment.[154] These takedown notice provisions provide a safe harbor for internet service providers who remove copyright infringing material following written notice of that infringing content.[155]

This Note, in contrast to these other proposals, advocates for an amendment to the CDA to permit lability for online intermediaries under a new federal cause of action for doxing.[156]

---

152. *See id*. ("[W]ithout a doubt the law represents a small crack in the CDA legal shield that had been undisturbed by Congress since it was passed in 1996.").

153. *See supra* note 143 and accompanying text (discussing the various proposals to amend § 230).

154. *See* Daniel J. Solove, *Speech, Privacy, and Reputation on the Internet*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 15, 26 (Saul Levmore & Martha C. Nussbaum eds., 2010) (proposing a CDA amendment with a DMCA-like takedown notice provision for defamation and privacy claims); Olivera Medenica & Kaiser Wahab, *Does Liability Enhance Credibility: Lessons from the DMCA Applied to Online Defamation*, 25 CARDOZO ARTS & ENT. L.J. 237, 239 (2007) (explaining that the DMCA can provide a model for an amendment to CDA § 230 for online defamation); Ariel Ronneburger, *Sex, Privacy, and Webpages: Creating a Legal Remedy for Victims of Porn 2.0*, 21 SYRACUSE SCI. & TECH. L. REP. 1, 4 (2009) (arguing the DMCA's takedown notice provision in DMCA Title II provides a model for an amendment to CDA § 230 to address the hosting of non-consensual pornographic videos or images); Bradley A. Areheart, *Regulating Cyberbullies Through Notice-Based Liability*, 117 YALE L.J. POCKET PART 41 (2007), https://www.yalelawjournal.org/forum/regulating-cyberbullies-through-notice-based-liability (articulating how some tortious cyberbullying could be regulated by amending the CDA with a DMCA-like notice and takedown provision); *cf. Website Design and Liability*, *supra* note 143, at 418 (proposing a "response-and-identification safe harbor" under which a "website operator may notify the poster and the poster may elect to stand by the posting by identifying herself. The posting would then become an 'identified' posting and the website operator would be immune from civil liability"); Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 409 (2005) (suggesting ISP reform that "implements the DMCA's safeguards against bad-faith or frivolous takedown requests").

155. *See* Ronneburger, *supra* note 154, at 24–28 (explaining the DMCA's takedown notice).

156. *Cf. id*. at 30 (arguing for an amendment to the CDA covering only revenge porn that is similar to the DMCA takedown notice provision, but not proposing any specific liability scheme in connection with the notice requirement).

The doxing amendment to the CDA should be modeled off the 2018 sex trafficking amendment.[157] Following the sex trafficking amendment, the doxing amendment could exclude from § 230 immunity violations of a new federal law on doxing that would cover both doxing and ghost doxing.[158]

Specifically, the doxing legislation should consist of three parts. First, a section that is similar to the proposed Online Safety Act.[159] Second, a section for websites that encourage or otherwise induce doxing that bases liability on a theory similar to copyright law's liability theory.[160] Third, the legislation should contain a section covering non-inducement doxing that could premise liability under a theory similar to copyright law's vicarious liability theory.[161] For this third section, online intermediaries could only be held liable if they received proper notice of doxing content and failed to remove it.[162] Overall, amending § 230 is a crucial first step

---

157. *See* 47 U.S.C. § 230(e)(5) (2012)

> Nothing in this section (other than subsection (c)(2)(A)) shall be construed to impair or limit—(A) any claim in a civil action brought under section 1959 of Title 18, if the conduct underlying the claim constitutes a violation of 1591 of that title; (B) any charge in a criminal prosecution brought under state law if the conduct underlying the charge would constitute a violation of section 1591 of Title 18; or (C) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 2421A of Title 18, and promotion or facilitation of prostitution is illegal in the jurisdiction where the defendant's promotion or facilitation of prostitution was targeted.

See also CITRON, *supra* note 22, at 177 (outlining a § 230 amendment that mirrors the existing federal criminal law and intellectual property exemptions).

158. *Cf.* Patrick J. Carome & Ari Holtzblatt, *Congress Enacts Law Creating a Sex Trafficking Exception from the Immunity Provided By Section 230 of the Communications Decency Act*, WILMERHALE, https://www.wilmerhale.com/en/insights/client-alerts/2018-04-16-congress-enacts-law-creating-a-sex-trafficking-exception-from-the-immunity-provided-by-section-230-of-the-communications-decency-act (last visited Sept. 16, 2019) (explaining the sex trafficking amendment excludes "from its [§ 230's] protection certain conduct that would constitute either a violation of federal sex trafficking laws or a criminal violation of the new federal criminal prostitution law") (on file with the Washington and Lee Law Review).

159. *See* H.R. 3067, 115th Cong. (2d Sess. 2017) (proposing criminal and civil liability for doxing).

160. *See infra* Part IV.

161. *See infra* Part IV.

162. *See infra* Part IV; *see also* CITRON, *supra* note 22, at 178 (articulating

to imposing liability on online intermediaries for doxing.

IV. An Analogy to Copyright Law's Secondary Liability Scheme

Once the § 230 immunity for online intermediaries excludes doxing, then one can determine the appropriate type of liability to impose. Copyright law provides a model for legislation to impose secondary liability on online intermediaries for ghost doxing.[163] The Copyright Act of 1976[164] does not address secondary liability, but the common law of copyright allows for secondary liability.[165] In copyright law there are two ways one can be held secondarily liable for copyright infringement: contributory infringement and vicarious infringement.[166] Contributory infringement occurs "by intentionally inducing or encouraging direct infringement."[167] Put another way, "one who, with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer."[168] Second, one "infringes vicariously by profiting from direct infringement" without stopping or limiting the direct infringement.[169] Vicarious liability was initially premised on

---

that her proposed § 230 amendment on nonconsensual pornography could also potentially include a safe harbor notice provision).

163. *See* CITRON, *supra* note 22, at 121–22 (noting copyright law can provide some recourse for cyber-harassment victims).

164. 17 U.S.C. §§ 101–810 (2012).

165. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 435 (1984) ("[T]he concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another.").

166. *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 929–30 (2005) (explaining secondary liability for infringement may be the only practical alternative when "it may be impossible to enforce the rights in the protected work effectively against all direct infringers").

167. *Id.* at 930.

168. *See* Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971) (stating the defendant knew that copyrighted works were performed at their association's venue and that "neither the local association nor the performing artists would secure a copyright license").

169. *See Grokster*, 545 U.S. at 930 (citing Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963) (describing vicarious liability in copyright).

agency law's *respondeat superior* doctrine,[170] but "even in the absence of an employer-employee relationship one may be vicariously liable if he has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities."[171] Thus, vicarious liability in copyright sometimes applies even when the entity lacks actual knowledge of the wrongful conduct.[172]

Just as copyright law provides two types of secondary liability, online intermediaries should be subject to two types of secondary liability for ghost doxing. First, online intermediaries that encourage or induce doxing should be held liable under reasoning similar to copyright's contributory infringement theory.[173] Second, online intermediaries that are not actively inducing or encouraging doxing should be held vicariously liable for ghost doxing if they fail to remove the doxed content after proper notice.[174]

A. Copyright's Secondary Liability Caselaw

The leading Supreme Court cases on secondary liability for copyright infringement are *Sony Corp. of America v. Universal Studios*[175] and *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*[176]

---

170. *See Gershwin*, 443 F.2d at 1162 (discussing how vicarious liability was originally premised on agency law).

171. *See id.* (arguing that in some instances the imposition of vicarious liability is appropriate).

172. *See* Shapiro, Bernstein & Co. v. H. L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963)

> When the right and ability to supervise coalesce with an obvious and direct financial interest in the exploitation of copyrighted materials—even in the absence of actual knowledge that the copyright monopoly is being impaired—the purpose of copyright law may be best effectuated by the imposition of liability upon the beneficiary of that exploitation.

173. *See infra* Part IV.A–B (explaining copyright law's secondary liability scheme).

174. *See infra* Part IV.A–B (describing how a notice provision is necessary to impose secondary liability in some instances).

175. 464 U.S. 417 (1984).

176. 545 U.S. 913 (2005).

In *Sony*, the Supreme Court considered imposing a claim of indirect infringement[177] based on the mere distribution of Betamax video tape recorders by Sony.[178] Universal Studios and Disney Productions owned the copyrights on many of the television programs that were taped by purchasers of Sony's Betamax recorders.[179] The purchasers creating the illegal copies were the "direct infringers," but the Court found Sony did not influence or encourage any of the illegal copies.[180] The Court reasoned "[i]f vicarious liability is to be imposed on petitioners in this case, it must rest on the fact that they have sold equipment with constructive knowledge of the fact that their customers may use that equipment to make unauthorized copies of copyrighted material."[181] The Supreme Court explained that the imposition of vicarious liability here—which was akin to strict liability for the end user conduct—was inappropriate.[182]

The Supreme Court then turned to the claim of contributory infringement.[183] It reasoned that "[t]he sale of other articles of commerce, [did] not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes."[184] Instead, the product need only "be capable of substantial noninfringing uses."[185] Since the Betamax videotape technology was capable of commercially significant noninfringing uses,[186]

---

177. "Indirect infringement" is an umbrella term for secondary liability for copyright infringement.

178. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 438 (1984) (discussing that the district court found that Sony did not induce any of the copies in question to be made).

179. *See id*. at 419, 421 (explaining Universal Studios and Walt Disney owned the copyrights for many motion pictures and other audiovisual works).

180. *See id*. at 438 (articulating the district court's finding that Sony did not have "either direct involvement with the allegedly infringing activity or direct contact with purchasers of Betamax who recorded copyright works off-the-air").

181. *Id*. at 439.

182. *See id*. ("There is no precedent in the law of copyright for the imposition of vicarious liability on such a theory.").

183. *See id*. (discussing how contributory liability in copyright law and patent law differ).

184. *Id*. at 442.

185. *Id.*

186. *See* Peter Menell & David Nimmer, *Unwinding Sony*, 95 CALIF. L. REV. 941, 942 (2007) (noting the commercially significant non-infringing uses in *Sony* were "time-shifting and the recording of public domain programming and

Sony was thus not liable for contributory infringement.[187]

Over twenty years later, the Court was again confronted with the issue of secondary liability for copyright infringement. In *Grokster*, various copyright holders—songwriters, music publishers, and motion picture studios (including MGM)—sued two peer-to-peer file sharing software distributors, StreamCast and Grokster ("Grokster"), for infringement.[188] The software functioned through decentralized peer-to-peer networks, which prevented Grokster from identifying which files were copied or when they were copied.[189] Evidence obtained in discovery, however, revealed that Grokster was aware that users primarily used its software to illegally download copyrighted files, and that Grokster intended and encouraged such uses.[190] MGM alleged that the software distributors "knowingly and intentionally distributed their software to enable users to infringe copyrighted works in violation of the Copyright Act," and sought damages and injunctive relief.[191]

Ultimately, the Supreme Court held "that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for resulting acts of infringement by third parties."[192] The Court rejected the Ninth Circuit's narrow reading of *Sony*,[193] which suggested "that whenever a product is

---

copyrighted broadcasts").

187. *See Sony*, 464 U.S. at 456 ("Sony's sale of such equipment to the general public does not constitute contributory infringement of respondent's copyrights.").

188. *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 919–20 (2005) (stating the software in question allows users to share files directly with one another without going through a central server).

189. *See id.* (describing how Grokster's software allows users to share electronic files through peer-to-peer networks).

190. *See id*. at 922 (discussing that MGM commissioned a systematic search and found that ninety percent of files available for download were copyrighted works).

191. *Id*. at 921.

192. *See id.* at 937 ("The inducement rule, instead, premises liability on purposeful, culpable expression and conduct, and thus does nothing to compromise legitimate commerce or discourage innovation having a lawful promise.").

193. *See id*. at 934 (explaining *Sony* "was never meant to foreclose rules of fault-based liability derived from the common law").

capable of substantial lawful use, the producer can never be held contributorily liable for third parties' infringing use of it."[194] In the Court's review, *Sony* does not "require courts to ignore evidence of intent if there is such evidence [of inducement], and the case was never meant to foreclose rules of fault-based liability derived from the common law."[195] The Supreme Court, however, took pains to make clear that *Grokster* did not overturn *Sony*.[196] Rather, *Grokster* underscored the importance of examining evidence of inducement when it is present, even if the product is capable of substantially non-infringing uses.[197]

B. Toward a Theory of Secondary Liability for Ghost Doxing

Copyright provides a useful secondary liability scheme that can be applied to ghost doxing.[198] First, online intermediaries that encourage doxing should be held liable under a contributory liability theory similar to copyright law. Second, online intermediaries that have non-inducement doxing on their site should be liable under a vicarious liability theory if they are given notice and fail to remove the content.

1. Contributory Liability for Encouraging Doxing

Similar to copyright law, online intermediaries could be held secondarily liable when they intentionally induce or encourage doxing. Just as Sony was not liable for infringement by users when its product had substantially non-infringing uses, it would be bad policy to hold online intermediaries liable for doxing when they do

194. *Id*.

195. *See id*. at 934–35 (noting *Sony* does not require courts to ignore evidence of inducement because a product is capable of substantial non-infringing use).

196. *See id*. at 934 (stating the Supreme Court intended "to leave further consideration of the *Sony* rule for a day when that may be required").

197. *See id*. at 937 ("We are, of course, mindful of the need to keep from trenching on regular commerce or discouraging the development of technologies with lawful and unlawful potential.").

198. *See supra* notes 49–57 and accompanying text (proposing copyright law's secondary liability scheme as a useful analogy for doxing); *see also* CITRON, *supra* note 22, at 121–22 (articulating copyright law could potentially provide recourse for cyber-harassment victims).

no more than provide discussion forums.[199] However, online intermediaries that encourage posting of personal information by ghost doxers or those that make victims pay for removing such information should be subject to contributory liability.[200] For example, various revenge porn websites advertise that they will remove content for a fee.[201] These types of websites encourage doxing and other forms of cyber-harassment and should be held liable for the doxing they encourage.[202] Encouragement could mean advertising for doxing or otherwise attempting to persuade third parties to dox.[203] Similar to the reasoning used in *Grokster*, a website that is encouraging doxing—even if it is capable of substantial non-doxing uses—could be held contributorily liable if there is evidence of doxing encouragement.[204] This secondary liability should be imposed even without a notice requirement if the online intermediary is encouraging the doxing.

---

199. *Cf.* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 456 (1984) (stating Sony's tape recorder product was capable of substantial non-infringing uses).

200. *See* CITRON, *supra* note 22, at 175 (discussing extortion sites that advertise for revenge porn and other damaging information, such as mug shots, and then turn around and profit from the removal of such content); Goldnick, *supra* note 22, at 627 (arguing the CDA could be amended for "ISPs and website operators/hosts who purposely proliferate or encourage the proliferation of revenge porn").

201. *See* CITRON, *supra* note 22, at 174 (outlining various revenge porn websites, gossip websites, and even mug shot removal websites that advertise a removal or takedown service for specified content for a fee). It is unclear if these types of websites have immunity under § 230 currently. *See id.* at 175 ("It is unclear whether Section 230's immunity extends to sites that effectively engage in extortion by encouraging the posting of sensitive private information and profiting from its removal.").

202. *See id.* at 175 (describing various websites that encourage different forms of cyber-harassment); Bartow, *supra* note 61, at 391–92 (stating that the entities who market themselves as able to assist those whose reputations have been attacked online have incentives to "oppose legal reforms that might enable online defamation and harassment victims to seek recourse").

203. *Cf.* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd, 545 U.S. 913, 927 (2005) ("StreamCast not only rejected another company's offer of help to monitor infringement . . . but blocked the Internet Protocol address of entities it believed were trying to engage in such monitoring on its networks.").

204. *Cf. id.* at 934–35 (articulating that even if a product is capable of substantial non-infringing uses, that does not mean a court must ignore evidence of inducement if it is present).

At least one circuit found an online service provider potentially liable for contributing to illegal conduct.[205] In *Fair Housing Council v. Roommates.com*,[206] the Ninth Circuit denied § 230 immunity to Roommates.com, an online roommate matching website, because the site "materially contributed" to the alleged violations of the Fair Housing Act and applicable state laws through the questionnaires the company required users to fill out.[207] The Ninth Circuit found that "Roommates's work in developing the discriminatory questions, discriminatory answers and discriminatory search mechanism [was] directly related to the alleged illegality of the site."[208] Similar to how Roommates.com could be held secondarily liable if it encouraged illegal discriminatory housing practices,[209] sites that encourage doxing should be held secondarily liable for doxing.

---

205. *See* Fair Hous. Council v. Roommates.com, 521 F.3d 1157, 1164 (9th Cir. 2008) (explaining because "Roommate created the questions and choice of answers, and designed its website registration process around them" the website was an "information content provider" for these questions, which allegedly violated the Fair Housing Act and state laws), *rev'd on other grounds*, 666 F.3d 1216 (9th Cir. 2012) (vacating the district court's judgment for plaintiff on remand because "Roommates' prompting, sorting and publishing of information to facilitate selection is not forbidden by" the applicable laws); Gallardo, *supra* note 80, at 738 (discussing the implications of the Ninth Circuit's *Roommates.com* case on § 230 immunity); *but see* Jones v. Dirty World Entm't Recordings, LLC, 755 F.3d 398, 401–03 (6th Cir. 2014) (stating how the Sixth Circuit said that an encouragement test was not the correct test for determining whether a website was eligible for immunity under CDA § 230).

206. 521 F.3d 1157 (9th Cir. 2008).

207. *See id.* at 1167–71 (finding an internet service provider that designed a website intended to solicit and enforce allegedly illegal housing preferences "materially contributed" to illegality and therefore was not entitled to immunity under § 230). The Ninth Circuit did find that the operator was entitled to immunity for the "Additional Comments" section of the website. *See id.* at 1174 (describing the "Additional Comments" section of the website as a "generic prompt [that] does not make [the site] a developer of the information posted").

208. *See id.* at 1172 ("Roommate is directly involved with developing and enforcing a system that subjects subscribers to allegedly discriminatory housing practices.").

209. *Contra* Fair Hous. Council v. Roommate.com, 666 F.3d 1216, 1224 (9th Cir. 2012) (articulating that on remand that the Ninth Circuit ultimately found Roommate not liable because the "prompting, sorting and publishing of information to facilitate roommate selection is not forbidden by the FHA" or the applicable state housing law).

2. Vicarious Liability for Non-Inducement Doxing

For online intermediaries not actively encouraging doxing, vicarious liability is more appropriate. Vicarious liability is arguably the more widely applicable form of secondary liability because online intermediaries do, typically, have the right and ability to control what is posted on their sites and have a financial interest in such activities.[210] While online intermediaries do have the right and ability to control what is posted on their sites, that does not mean it is reasonable to expect them to "police" the internet for harms created by others using their platform.[211] Therefore, when there is non-induced doxing activity on a website, an online intermediary should be held secondarily liable if it fails to remove doxing content after receiving proper notice.[212]

3. How the DMCA's Notice Provision Can Be Applied to Ghost Doxing

Copyright law, through the DMCA, provides a useful framework for a notice and takedown provision that can be applied to doxing.[213] The DMCA provides safe harbors for online service providers that insulate them from copyright liability if they comply with the statutory provisions.[214] The safe harbor provisions of the DMCA reflect the idea that an online service provider "cannot be held liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material."[215] Following this same logic, DMCA § 512(c)'s takedown

---

210. *See* CITRON, *supra* note 22, at 180 (explaining in some situations it is in the interest of a website to keep up material that attracts viewers and advertising revenue).

211. *See* SOLOVE, *supra* note 129, at 152 (discussing how it is unrealistic for online intermediaries to police all the content on their sites).

212. *See infra* Part IV.B.3 (arguing the DMCA can provide a model for a parallel anti-doxing notice and takedown provision).

213. *See supra* notes 153–155, 161–162 and accompanying text (describing how the DMCA could be used as a model for a cyber-harassment regulatory notice provision).

214. *See* 17 U.S.C. § 512(a)–(d) (2012) (outlining the four safe harbor provisions for service providers).

215. UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1021 (9th Cir. 2013) (quoting A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004,

notice provision provides an excellent model for a notice requirement that could be applied to an online intermediary with ghost doxing on its site.

Under the DMCA, a service provider must meet certain threshold criteria to qualify for the safe harbor provisions.[216] First, the party must be a "service provider," as defined in the statute.[217] Second, a party must satisfy "conditions of eligibility."[218] Conditions of eligibility for service providers include: enforcing a "repeat infringer" policy that terminates subscribers and account holders who repeatedly infringe copyrights[219] and not interfering with technical measures "used by copyright owners to identify or protect copyrighted works."[220] Third, a service provider must designate an agent publicly to receive notice of alleged infringements.[221]

A qualified service provider must also meet the criteria outlined within the specific safe harbor provision.[222] Under § 512(c)(1), safe harbor from secondary liability for infringement is only available if the service provider:

- Does not have actual knowledge of infringing material,[223]

1021 (9th Cir. 2001)).

216. *See* Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 27 (2d Cir. 2012) (discussing the threshold requirements for service providers to qualify for DMCA safe harbor).

217. *See* 17 U.S.C. § 512(k)(1)(b) (defining service provider as "a provider of online services or network access, or the operator of facilities therefor").

218. *See id.* § 512(i)(1)(A) (listing conditions of eligibility).

219. *Id.*

220. *See id.* §§ 512(i)(1)(B), 512(i)(2) (articulating conditions of eligibility and defining standard technical measures).

221. *See id.* § 512(c)(2) (stating information about an agent should include at least their name, address, phone number, and electronic mail address and must be made available publicly).

222. *See id.* § 512(a)–(d) (outlining the four safe harbor provisions for service providers). Subsection (l) states a failure to qualify for a limitation of liability under this section does not affect the consideration of a defense by the service provider that they did not engage in infringing conduct. *Id.* § 512(l); *see also Viacom,* 676 F.3d at 27 (discussing how each of the four DMCA safe harbor provisions have slightly different criteria).

223. 17 U.S.C. § 512(c)(1)(A)(i) (2012).

  - Does not have "red flag" knowledge,[224] or
  - Upon obtaining knowledge or "red flag" knowledge acts to remove or disable access to the notified material;[225]
- "Does not receive a financial benefit directly attributable to the infringing activity" when "the service provider has the right and ability to control such activity;"[226] and
- When proper notice of infringing material is given, the service provider removes or disables access to the material in a timely manner.[227]

Courts have distinguished between actual knowledge[228] and so-called "red flag" knowledge.[229]

Viacom International, Inc. v. YouTube, Inc.[230] is a key case that applies § 512(c)'s safe harbor provision.[231] The plaintiffs in *Viacom* alleged direct and secondary copyright infringement "based on the public performance, display, and reproduction of approximately 79,000 audiovisual 'clips' that appeared on the YouTube website between 2005 and 2008."[232] The defendant YouTube argued it was within the safe harbor.[233] The Second Circuit held that for a service provider to have actual knowledge or so-called "red flag" knowledge, it must be aware of "specific and

---

224. *Id.* § 512(c)(1)(A)(ii).

225. *Id.* § 512(c)(1)(A)(iii).

226. *Id.* § 512(c)(1)(B); *see also Viacom*, 676 F.3d at 38 (explaining the benefit and control provision requires more than the ability to remove or block material, but also acknowledging "something more" is difficult to define).

227. 17 U.S.C. § 512(c)(1)(C).

228. *Id.* § 512(c)(1)(A)(i).

229. *Id.* § 512(c)(1)(A)(ii); *see* Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2d Cir. 2012) (clarifying the nuances of actual knowledge and red flag knowledge in § 512(c)); UMG Recordings, Inc. v. Shelter Capital Partners, LLC, 718 F.3d 1006, 1023 (9th Cir. 2013) (explaining the § 512(c) safe harbor provisions for actual knowledge and red flag knowledge both require the service provider to know of instances of infringing conduct).

230. 676 F.3d 19 (2d Cir. 2012).

231. *See id.* at 26 (concluding the "§ 512(c) safe harbor requires knowledge or awareness of specific infringing activity").

232. *Id.* The clips included Bud Light commercials and Premier League games. *Id.* at 33–34.

233. *See id.* at 26 (discussing whether YouTube was within the § 512(c) safe harbor).

identifiable infringing activity."[234] The court vacated the summary judgment order in favor of YouTube "because a reasonable jury could find that YouTube had actual knowledge or awareness of specific infringing activity on its website."[235] If the relevant decision makers at YouTube did in fact have that knowledge, then that knowledge triggered an obligation for the site to remove the infringing material in a timely manner.[236] On remand, however, the court found the safe harbor applied and granted YouTube's motion for summary judgment.[237]

The DMCA's takedown notice requirement should be applied to doxing.[238] Under the DMCA, the takedown notice must be written and provided to the service provider's designated agent.[239] The notice must include a signature of the person authorized to act on behalf of the copyright owner; identification of the infringed copyright work or works; enough information to allow the service provider to contact the complaining party; a statement that the notification is accurate under penalty of perjury and that the complainant is authorized to act on behalf of the copyright owner; and that the complaining party has a good faith belief that the material being complained about is not an authorized use.[240] If proper takedown notice is provided, the service provider is required to "act expeditiously" to remove the material.[241] This takedown notice provision is used often. For example, Google has

---

234. *Id*.

235. *Id.* Emails between relevant YouTube decision makers discussed specific infringing content, such as Premier League games and Bud Light commercials, that allegedly remained on the site following the email discussions. *Id.* at 33–34.

236. *See id.* at 27–28 (articulating that once knowledge is established, the service provider must then timely remove the infringing content).

237. *See* Viacom Int'l, Inc. v. YouTube, Inc., 940 F. Supp. 2d 110, 123 (S.D.N.Y. 2013) (conveying YouTube was within the § 512(c) safe harbor).

238. *Cf.* 17 U.S.C. § 512(c)(3) (2012) (listing the elements of proper notice and explaining what a service provider must do if given proper notice).

239. *See id.* § 512(c)(3)(A) (providing details on the takedown notice provision).

240. *See id*. § 512(c)(3)(A)(i)–(vi) (detailing the requirements of a proper takedown notice under the DMCA).

241. *Id.* § 512(c); *see* Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 27–28 (2d Cir. 2012) ("[A]ctual knowledge of infringing material, awareness of facts or circumstances that make infringing activity apparent, or receipt of a takedown notice will each trigger an obligation to expeditiously remove the infringing material.").

a tracking service—Google Transparency Report—that provides an ongoing tally of URLs for which the site has received takedown notice notifications.[242]

A vicarious liability scheme coupled with a notice provision could provide the outline of a ghost doxing liability statute for non-inducement doxing. Specifically, the ghost doxing notice and takedown provision could parallel the DMCA § 512(c).[243] The ghost doxing provision should require online intermediaries to designate an agent to receive notice of doxing content.[244] The takedown notice specifics in § 512(c)(3) should also be used as a model as they provide specific instructions for notifying an intermediary of doxing content.[245]

Experience has shown that it is unrealistic to assume that online intermediaries will unilaterally police the internet to prevent doxing.[246] Thus, this Note does not propose legislation that places an affirmative duty on online intermediaries to seek out and eliminate instances of doxing.[247] Further, the DMCA's good faith belief component would also be crucial to incorporate into a parallel anti-doxing notice and takedown provision. Requiring a good faith belief by the complainant that the content posting constitutes doxing will help prevent complaints by those who simply disagree with the content of the reported post.[248] Overall, a

---

242. *See Transparency Report*, GOOGLE, https://transparencyreport.google.com/copyright/overview?hl=en (last visited Sept. 8, 2019) (listing the number of URLs submitted for delisting as of September 8, 2019 at 4,243,160,549) (on file with the Washington and Lee Law Review).

243. *See* 17 U.S.C. § 512(c)(1)(C) (requiring notice and timely takedown for a service provider to be within the safe harbor provision).

244. *See id*. § 512(c)(2) (noting a designated agent's contact information must be publicly available).

245. *See id*. § 512(c)(3)(A)(i)–(vi) (outlining the requirements for DMCA takedown notice).

246. *See* Rustad & Keonig, *supra* note 154, at 351 ("ISPs currently have no duty to police the Internet or to develop technologies to track down off-shore posters of objectionable materials.").

247. *Cf*. § 512(m) (stating the applicability of § 512(a)–(d) is not conditioned on "a service provider monitoring its service or affirmatively seeking facts indicating infringing activity").

248. *See* CITRON, *supra* note 22, at 179 (explaining the "heckler's veto" concept, which says that "people will complain about speech because they dislike the speakers or object to their views, not because they have suffered actual harm").

notice provision similar to DMCA will provide the online intermediary an opportunity to remove the doxing content in a timely manner and be immunized if they comply.

V. Conclusion

Doxing is a growing problem that causes harm in the real "offline" world. The law needs to be updated to address modern harms like doxing. The outdated blanket immunity of the CDA § 230 should be narrowed to be more in line with the realities of today's internet and allow online intermediaries to potentially be held liable in limited circumstances for doxing. To adequately address doxing, however, amending the CDA is not enough. Congress also needs to pass legislation that directly addresses both doxing and ghost doxing. Specifically, Congress should pass legislation similar to the proposed Online Safety Act, but also amend that legislation to include two new sections that address ghost doxing.

To address ghost doxing, copyright law provides a persuasive analogy for imposing secondary liability on online intermediaries. Online intermediaries that intentionally induce or encourage doxing should be held secondarily liable under a contributory theory that is similar to contributory infringement under copyright law. Vicarious liability, however, is a more appropriate type of secondary liability for an online intermediary that is not actively inducing doxing. An online intermediary should not be held vicariously liable unless it was given proper notice of the doxing content and failed to remove it. Society should no longer allow online intermediaries to avoid liability for the legitimate harms done by doxing.