Washington and Lee Law Review

Volume 71 | Issue 4 Article 9

Fall 9-1-2014

Taking Back the Internet: Imposing Civil Liability on Interactive Computer Services in an Attempt to Provide an Adequate Remedy to Victims of Nonconsensual Pornography

Amanda L. Cecil
Washington and Lee University School of Law

Taking Back the Internet: Imposing Civil Liability on Interactive Computer Services in an Attempt to Provide an Adequate Remedy to Victims of Nonconsensual Pornography

Amanda L. Cecil*

Table of Contents

* J.D. candidate, Washington and Lee University School of Law, May 2015. I would like to thank professors Johanna Bond and Brian Murchison for the invaluable feedback that they provided throughout the writing process. I would also like to thank my parents for their unending encouragement, as well as the friends and family that have supported me along the way.

I. Introduction

At the age of thirty-three, Hollie Toups received a life-changing phone call.[1] While at work, the Texas teacher's aide answered her phone only to hear the devastating news that half-naked images from her past could be found online.[2] After rushing home to check the website Texxxan.com, Hollie discovered several topless photographs of herself.[3] She had taken the photographs nearly ten years earlier for an ex-boyfriend,[4] and now they flashed across her computer screen with links attached to her social media accounts and a Google map of her location.[5] Both humiliated and afraid, Hollie refused to leave her home for days, and when she finally ventured into town, strange men approached her about the seminude photographs.[6] Unwilling to

1. *See* James Fletcher, *The Revenge Porn Avengers*, BBC NEWS, http://www.bbc.co.uk/news/magazine-25321301 (last updated Dec. 11, 2013, 2:25 PM) (last visited Nov. 18, 2014) (interviewing Hollie Toups and detailing her experience as a revenge porn victim) (on file with the Washington and Lee Law Review); *Women's Outrage After Ex-Boyfriends Post Revenge Porn Photos*, ABC NEWS (Jan. 25, 2013, 8:34 AM), http://abcnews.go.com/blogs/headlines/2013/01/womens-outrage-after-ex-boyfriends-post-nude-photos/ (last visited Nov. 18, 2014) [hereinafter *Women's Outrage*] (discussing the stories of several revenge porn victims, including Hollie Toups's story) (on file with the Washington and Lee Law Review).

2. *See* Fletcher, *supra* note 1 (recounting the details of the day Hollie Toups discovered her own seminude photographs on Texxxan.com).

3. *See id.* (explaining that Toups left work, went directly home, and "ran upstairs and opened [her] computer," where she discovered topless photographs of herself on Texxxan.com).

4. *See id.* (noting that the thirty-three-year-old had taken the photos for an ex-boyfriend when she was twenty-four).

5. *See id.* (noting that the topless images appeared with Toups's name, links to her Facebook and Twitter accounts, a Google map of her location, and a stream of user comments).

6. *See id.* ("She was afraid to leave the house, and when she eventually

accept this devastating form of public humiliation, Hollie chose to fight Texxxan.com.[7] Ultimately, her legal battle would gain national attention and bring light to the legal issues surrounding the nonconsensual distribution of sexually explicit images of an ex-partner,[8] now commonly known as "revenge porn."[9]

Hollie's story is not unlike those of countless other revenge porn victims.[10] Because she originally captured the images for a romantic interest, Hollie assumed her ex-boyfriend distributed the pictures.[11] Though she eventually discovered that a hacker stole the images from her phone,[12] Hollie's first assumption illustrates the common principle behind revenge porn. Most images found on revenge porn websites stem from ex-partners, jilted by their former partner and seeking revenge through public humiliation.[13] If an ex-partner stores sexually explicit photographs from the relationship, the ex-partner may distribute these to various revenge porn distribution websites.[14] Once the

---

did, she was approached several times by men who had seen the photos.").

7. *See id.* (noting that Hollie Toups and "dozens of other women" filed a class action civil lawsuit against the website owners, the web-hosting company, and even some of the original posters for invasion of privacy); *Women's Outrage*, *supra* note 1 (noting that Hollie Toups and other victims attempted to "reclaim their privacy" by pursuing claims against Texxxan.com and its host server, GoDaddy.com).

8. *See* Derek Bambauer, *Beating Revenge Porn with Copyright*, INFO/LAW BLOG (Jan. 25, 2013), https://blogs.law.harvard.edu/infolaw/2013/01/25/beating-revenge-porn-with-copyright/ (last visited Nov. 18, 2014) [hereinafter Bambauer, *Beating Revenge Porn with Copyright*] ("The lawsuit against scumbag Web site Texxxan.com has generated attention to the problem of revenge porn, and to the paucity of legal remedies available to victims of it.") (on file with the Washington and Lee Law Review).

9. *See infra* note 45 and accompanying text (defining revenge porn).

10. *See, e.g.*, Fletcher, *supra* note 1 ("[T]he experience of Hollie Toups and other women is typical of victims everywhere . . . .").

11. *See, e.g.*, *id.* (noting that Toups originally suspected that her ex-boyfriend posted the photographs).

12. *See, e.g.*, *id.* (explaining that because some of her revenge porn photographs had never been shared with anyone, Hollie Toups believes a cell phone repair service hacked the images).

13. *See, e.g.*, *infra* note 45 and accompanying text (explaining that revenge porn usually appears after a romantic relationship ends and one partner shares sexually explicit images that were created during the relationship).

14. *See* Mary Anne Franks, Combating Non-Consensual Pornography: A Working Paper 3 (Dec. 5, 2013) (unpublished manuscript) [hereinafter Franks,

images find their way to a site, either through vengeful ex-partners or thieving hackers, they become extremely difficult to remove.[15]

Hollie Toups understood well the legal barriers surrounding the removal of these images. After discovering her seminude photographs online and desperately seeking a way to remove them, Hollie reached out to local law enforcement and legal services.[16] She found little aid in the police officers and attorneys who told her that there was nothing she could do and often scolded her for taking the pictures.[17] Finally, Hollie began working with local private investigators who were able to shut the site down on child pornography charges because some photos on the site displayed women under the age of eighteen.[18] With few other legal options remaining,[19] Hollie and several other victims filed a class action invasion-of-privacy suit against the owners of Texxxan.com and its web-hosting company, GoDaddy.com.[20]

A Working Paper] (explaining that an ex-partner or hacker may upload the sexually explicit images to a website, allowing thousands of people to view the images) (on file with the Washington and Lee Law Review).

15. *See* Lorelei Laird, *Victims Are Taking on "Revenge Porn" Websites for Posting Photos They Didn't Consent To*, A.B.A. J. (Nov. 1, 2013, 9:30 AM), http://www.abajournal.com/magazine/article/victims_are_taking_on_revenge_porn_websites_for_posting_photos_they_didnt_c/?utm_source=maestro&utm_medium=email&utm_campaign=tech_monthly (last visited Nov. 18, 2014) (noting that there is no clear legal avenue to penalize revenge porn posters and many victims are turned away by law enforcement) (on file with the Washington and Lee Law Review).

16. *See* Fletcher, *supra* note 1 (explaining that many women in Toups's town fell victim to similar revenge porn schemes and most attempted to notify law enforcement or find an attorney).

17. *See id.* ("[T]he response [from police and lawyers] was generally the same—they were told there was nothing they could do, and they shouldn't have taken the photos in the first place.").

18. *See id.* (explaining that some of the photos displayed women under the age of eighteen and that the allegations of child pornography convinced operators to shut down the site).

19. *See infra* Part III (discussing a victim's available legal options).

20. *See* GoDaddy.com, LLC v. Toups, 429 S.W.3d 752, 753 (Tex. App. 2014) (reciting facts of the case).

Unfortunately, under § 230 of the Communications Decency Act (CDA),[21] website operators and their Internet Service Providers (ISPs) generally hold far-reaching immunity from the actions of third-party posters.[22] This provision allows revenge porn websites and their hosts to retain immunity from the actions of the individuals who post the images so long as the website did not create or develop the material.[23] When Hollie filed the class action suit against GoDaddy.com, the web-hosting company filed a motion to dismiss, citing its immunity under § 230.[24] The trial court denied the dismissal, but the Court of Appeals of Texas reversed the order: "Allowing plaintiffs' [sic] to assert any cause of action against GoDaddy for publishing content created by a third party, or for refusing to remove content created by a third party would be squarely inconsistent with section 230."[25]

Despite the outcome, the publicity from the case gained the attention of many state legislatures who have become increasingly aware of the inadequate legal options available to revenge porn victims.[26] For example, several states, including California, Maryland, and Wisconsin, passed anti-revenge-porn laws that provide varying degrees of protection for victims,[27] and

---

21. 47 U.S.C. § 230 (2012).

22. *See id.* § 230(c)(1) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

23. *Id.*

24. *See GoDaddy.com*, 429 S.W.3d at 753 (reciting procedural history of the case).

25. *Id.* at 758.

26. *See, e.g.*, Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 357–61 (2014) (explaining a revenge porn victim's civil and criminal law options and legal limitations); Franks, A Working Paper, *supra* note 14, at 4–7 (discussing the inadequacy of existing civil claims and criminal law); *infra* Part III (discussing existing legal options in greater detail).

27. *See* CAL. PENAL CODE § 647(j)(4)(A) (West 2013), *amended by* 2014 Cal. Legis. Serv. Ch. 71 (S.B. 1304) (West) (prohibiting the recording and subsequent nonconsensual distribution of images of intimate body parts of another identifiable individual when the parties understand that the images are to remain private); H.R. 43, 434th Gen. Assemb. (Md. 2014) (to be codified at MD. CODE, CRIM. LAW § 3-809) ("A person may not knowingly disclose [an image] of another person whose intimate parts are exposed or who is engaged in an act of sexual contact, without the consent of the other person and with the intent to

several other states quickly followed with their own anti-revenge-porn bills.[28] However, state legislation often faces serious constitutional challenges because critics claim the free speech rights of posters must be protected.[29] Critics argue that these state laws are overly broad and may censor merely offensive speech and speech on matters of public concern.[30] This criticism severely limited the California law, which now requires the victim to prove severe emotional damage.[31] As other states struggle to provide adequate legal remedies and avoid constitutional challenges, vengeful ex-partners continue to post illicit images, and website operators continue to receive immunity under § 230, leaving victims with limited legal options.[32]

This Note explores the legal issues surrounding revenge porn as well as the inadequate legal options available to victims; ultimately, it argues that reform of § 230 of the CDA can provide victims of revenge porn with a proper legal remedy.[33] Part II

---

cause serious emotional distress."); WIS. STAT. ANN. § 942.09 (West 2014) (prohibiting the transmission or distribution of nude or partially nude images without the consent of the photographed individual, regardless of whether the depicted individual consented to taking the photographs).

28. *See, e.g.*, S. 5949, 236th Leg., 2013–2014 Reg. Sess. (N.Y. 2013) (establishing "the crime of non-consensual disclosure of sexually explicit images as a class A misdemeanor"). This New York bill passed the state senate in June 2014 and awaits approval by the state assembly. *See also* H.R. 475, 116th Reg. Sess. (Fla. 2014) (prohibiting the intentional nonconsensual disclosure of a private, sexually explicit image of an individual who is identified through personal identifiers, links, or facial recognition for the purposes of harassment). This Florida bill died in committee on May 2, 2014.

29. *See infra* Part III.D (discussing the constitutional issues involved in state regulation of revenge porn).

30. *See* Derek E. Bambauer, *Exposed*, 98 MINN. L. REV. 2025, 2088 (2014) [hereinafter Bambauer, *Exposed*] (explaining why criminal sanctions against nonconsensual distribution of images may face First Amendment scrutiny); Amanda Levendowski, *Using Copyright to Combat Revenge Porn*, 3 N.Y.U. J. INTELL. PROP. & ENT. L. 422, 438 (2014) ("From a First Amendment perspective, targeted revenge porn legislation occupies a tricky space: imprecisely drafted revenge porn legislation protects many victims but risks criminalizing protected expression, but whittling down legislation to avoid trammeling free speech excludes many of the victims the law intended to protect.").

31. *See* CAL. PENAL CODE § 647(j)(4)(A) (explaining that the author of the images must intend to cause, and must cause, "serious emotional distress").

32. *See infra* Part IV (discussing the § 230 limitations of state legislation).

33. *See infra* Part V (explaining why reform to § 230 may be the best

explains the rising trend of revenge porn as well as its devastating effects.[34] Part III explores a victim's existing legal options, including copyright law, tort law, criminal law, and state anti-revenge-porn legislation.[35] Part III also explains the inadequacies of these options, including the constitutional limitations of state legislation.[36] Part IV details the obstacle of § 230 immunity,[37] and it further clarifies why civil suits against revenge porn websites fail, leaving victims with little recourse.[38] Part V suggests that the most powerful and effective solution lies not in state legislation but in reform of § 230 of the CDA.[39] To reach this conclusion, it explores the recent movement away from traditional interpretations of § 230 immunity.[40] It then proposes the addition of takedown notice requirements that would allow victims to notify website operators of the images and request removal.[41] These provisions can limit the liability of website operators and ISPs without chilling communication on the Internet.[42] The Note concludes by highlighting the importance of setting an important federal standard for combating cyber harassment.[43]

---

available option for victims of revenge porn).

34. *See infra* Part II (defining revenge porn and explaining the challenges faced by victims).

35. *See infra* Part III (discussing existing legal options available to revenge porn victims).

36. *See infra* Part III.D (explaining the limitations to state anti-revenge-porn legislation).

37. *See infra* Part IV (explaining § 230 immunity).

38. *See infra* Part IV.B (explaining that traditional § 230 jurisprudence provides broad immunity to interactive computer services).

39. *See infra* Part V (proposing a solution to revenge porn that requires reform to § 230 of the CDA).

40. *See infra* Part IV.C (explaining case law that suggests a movement away from traditional interpretations of § 230 immunity).

41. *See infra* Part V.A (comparing § 230 of the CDA to the Digital Millennium Copyright Act and suggesting similar takedown notice procedures).

42. *See infra* Part V.C (explaining why takedown notice provisions in § 230 limit the immunity of ISPs without encouraging censorship).

43. *See infra* Part VI (discussing the implications of the proposed amendment).

II. Defining Revenge Porn

Revenge porn, or "involuntary pornography,"[44] involves the distribution of nude or sexually explicit photographs or videos of an individual without that individual's consent.[45] These sexually explicit images include photographs and videos taken by the victim, as well as images taken by the poster or another.[46] Though hackers sometimes obtain and distribute the images, the photos often surface after a romantic relationship.[47] The victim willingly provides the photos with the trust and confidence that they remain within the boundaries of the romantic relationship; however, once the relationship ends—perhaps on hateful terms—the partner holding the images seeks "revenge" by posting the material online.[48] Regardless of how the posters acquire the images, various outlets exist for the distribution of revenge porn. Websites such as UGotPosted,[49]

---

44. *See* Laird, *supra* note 15 (referring to the distribution of nude or sexually explicit photos as "revenge porn" or "involuntary pornography").

45. *See, e.g.*, Mary Anne Franks, *Unwilling Avatars: Idealism and Discrimination in Cyberspace*, 20 COLUM. J. GENDER & L. 224, 227 (2011) [hereinafter Franks, *Unwilling Avatars*] (defining revenge porn as "a practice where ex-boyfriends and husbands post to the web sexually explicit photographs and videos of [women] without their consent"); Laird, *supra* note 15 (defining revenge porn as "nude or sexual photos posted online without [the victim's] consent"); Suneal Bedi, *California's Attempt to Avenge Revenge Porn*, HUFFINGTON POST (Oct. 8, 2013, 11:21 AM), http://www.huffingtonpost.com/suneal-bedi/california-revenge-porn_b_3879916.html (last updated Nov. 9, 2013, 5:12 AM) (last visited Nov. 18, 2014) (defining revenge porn as the act of distributing nude or seminude photos or videos of an individual without that individual's consent) (on file with the Washington and Lee Law Review).

46. *See* MARY ANNE FRANKS, CRIMINALIZING REVENGE PORN: FREQUENTLY ASKED QUESTIONS (Oct. 9, 2013) [hereinafter FRANKS, FREQUENTLY ASKED QUESTIONS], *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2337998 (defining revenge porn).

47. *See, e.g.*, Fletcher, *supra* note 1 (explaining that the name "revenge porn" implies that most of the sexually explicit images appear online as a form of revenge after a relationship ends); Laird, *supra* note 15 ("Revenge porn gets its name because many pictures are posted by former lovers who kept sexual photos after the relationship ended. Others are reportedly acquired through hacking, theft by repair people or false personal ads.").

48. *See* Laird, *supra* note 15 (explaining that revenge porn often stems from former lovers that seek revenge on their ex-partners).

49. *See* Dan Thompson, *Man Who Ran 'Revenge Porn' Site Ugotposted.Com Charged After Allegedly Extorting Tens of Thousands of Dollars From Victims*,

IsAnyoneUp.com,[50] and Texxxan.com[51] allow visitors to post pornographic photographs and videos of their ex-partners and others, advertising "payback" against the exes that jilted them.[52]

As revenge porn distribution websites increase in number and popularity, revenge porn spreads more rapidly across the Internet and around the world.[53] Less than five years ago, websites like IsAnyoneUp.com and Texxxan.com did not exist; rather, individuals circulated sexually explicit images of their former partners through e-mail or maybe the occasional blog.[54] Early in the Internet age and before the explosion of revenge porn distribution websites, these photos could be quickly and quietly

---

NAT'L POST (Dec. 11, 2013, 4:02 PM), http://news.nationalpost.com/2013/12/11/man-who-ran-revenge-porn-site-ugotposted-com-charged-after-allegedly-extorting-tens-of-thousands-of-dollars-from-victims/ (last visited Nov. 18, 2014) (reporting the arrest of the owner of UGotPosted, a revenge porn website that required submissions identify victims by name, age, and other identifying information) (on file with the Washington and Lee Law Review).

50. *See* Lee Moran, *Revenge Porn Website IsAnyoneUp.com Shut Down After Anti-Bullying Group Buys Domain Name*, DAILY MAIL ONLINE (Apr. 20, 2012, 8:59 AM), http://www.dailymail.co.uk/news/article-2132672/Revenge-porn-website-IsAnyoneUp-com-shut-anti-bullying-group-buys-domain---new-owner-slammed-running-VERY-similar-service.html (last visited Nov. 18, 2014) (reporting the shutdown of revenge porn website IsAnyoneUp.com) (on file with the Washington and Lee Law Review).

51. *See "Revenge Porn" Website Featuring Half-Naked Photos that Is Facing Lawsuit Gets Shut Down By Host Site*, DAILY MAIL ONLINE (Feb. 5, 2013, 5:11 PM), http://www.dailymail.co.uk/news/article-2274099/Revenge-porn-website-texxxan-com-featuring-womens-half-naked-photos-sued-gets-shut-host-site.html (last visited Nov. 18, 2014) (reporting the shutdown of Texxxan.com) (on file with the Washington and Lee Law Review).

52. *See id.* (noting that sites like Texxxan.com are referred to as revenge porn because so many of the images are shared by "jilted ex-lovers" with the purpose of degrading the victims).

53. *See* Bambauer, *Exposed*, *supra* note 30, at 2034 (explaining statistics that show a desire to share intimate photographs with a romantic partner has increased, as has the unauthorized distribution of such images (citations omitted)); Citron & Franks, *supra* note 26, at 350 ("Today, intimate photographs are increasingly being distributed online, potentially reaching thousands, even millions of people, with a click of a mouse.").

54. *See* Laird, *supra* note 15 (naming two attorneys who started representing revenge porn victims four years ago, before the creation of revenge porn distribution sites, and noting that their clients' photos were usually sent through e-mail or posted on photo-sharing sites or blogs).

contained.[55] Today, however, websites like IsAnyoneUp.com and others exist with the intent of distributing these photos and humiliating the victims,[56] and the photos are no longer removed upon request.[57] Despite these concerns, more and more individuals share nude or suggestive photos with their partners,[58] and unfortunately, more and more partners betray that confidence and distribute those images across the Internet.[59]

As the popularity of revenge porn grows, so does the harm caused by this unique form of cyber harassment. Because revenge porn usually carries identifying information about the victim and links to his or her social networking profile,[60] the sexually explicit

---

55. *See id.* ("Before the Internet . . . compromising photos could do limited harm because they stayed within a few people's hands. Earlier in the Internet era, online photo-sharing sites would take them down quickly if asked.").

56. *See id.* (describing the purpose of the sites as an intent to "publicly shame, humiliate and degrade the victim"); Jill Filipovic, *"Revenge Porn" Is About Degrading Women Sexually and Professionally*, THE GUARDIAN (Jan. 28, 2013, 5:23 PM), http://www.theguardian.com/commentisfree/2013/jan/28/revenge-porn-degrades-women (last visited Nov. 18, 2014) ("[The sites] aren't about naked girls; there are plenty of those who are on the internet consensually. It's about hating women, taking enjoyment in seeing them violated, and harming them.") (on file with the Washington and Lee Law Review).

57. *See, e.g.*, Bekah Wells, *An Involuntary Porn Star: My Story*, WOMEN AGAINST REVENGE PORN, http://www.womenagainstrevengeporn.com/#!An-Involuntary-Pornstar-My-Story-/c618/6151C735-CEEF-45B2-A175-AC3E61347B3A (last visited Nov. 18, 2014) (recalling how Wells's own cease-and-desist letter was simply ignored) (on file with the Washington and Lee Law Review). *But see* Part III.A (explaining that some victims may seek removal through copyright law).

58. *See* Bambauer, *Exposed*, *supra* note 30, at 2034–45 (citing surveys that reveal 53.5% of heterosexual respondents and 74.8% of lesbian, gay, bisexual, and transgender respondents shared a nude photo with another, while another study reveals that nearly one-third of young adults ages twenty to twenty-six have posted or sent nude images of themselves).

59. *See id.* at 2028 ("People increasingly share intimate media—nude or sexually explicit photos or videos—with their partners. And those partners increasingly betray that trust by sharing those media without consent.").

60. *See* Laird, *supra* note 15 ("Involuntary porn is generally posted with the subject's real name, city and state, and often links to social media profiles."). For example, Bekah Wells discovered nude photographs of herself on a revenge porn site after randomly Googling her own name. Wells, *supra* note 57. The photos listed not only her name but also her city and occupation. *Id.* Similarly, the photographs of Hollie Toups also listed her name and provided a link to her Facebook profile. Bambauer, *Exposed*, *supra* note 30, at 2026 (citation omitted).

images begin to appear frequently as top search results on Google and other Internet search engines.[61] In a digital age where employers and educational institutions depend on Google searches and social media profiles to facilitate hiring or admissions processes,[62] such search results prove truly devastating to a victim's professional life.[63] When the images also include contact information for the victim's family and friends, the harm extends into the victim's personal life as well.[64]

Because the photos remain in the unforgiving realm of cyberspace and cannot be easily removed from revenge porn websites, the harm proves severe and long-lasting.[65] Victims may try to confine the harm by deleting their online presence, but they isolate themselves from rewarding social connections and personal contacts, limiting their friendships and dating opportunities.[66] Offline, the victims completely alter their lives in

---

61. *See* Laird, *supra* note 15 (explaining that posting the images with identifying information "helps get the pictures high in Google search results for the subject's name," which "hurts the victim's ability to get or keep jobs, dates and more").

62. *See* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 80 (2009) ("Employers often review Google searches before interviewing and hiring candidates."); Citron & Franks, *supra* note 26, at 352 (referring to a study that indicates nearly 80% of employers use Internet search engines to research job applicants, rejecting about 70% of applicants based on their findings (citation omitted)).

63. *See, e.g.*, Citron, *supra* note 62, at 70–71 (explaining that because many comments are damaging to the victim's reputation, spread false claims about mental illness and physical disease, and are often forwarded directly to employers, these comments may interfere with economic opportunities); Citron & Franks, *supra* note 26, at 350–54 (explaining the adverse impact of revenge porn, including physical stress, economic repercussions, and sexual assaults).

64. *See* Citron & Franks, *supra* note 26, at 350 ("[The image] can be e-mailed or otherwise exhibited to the victim's family, employees, co-workers, and friends."); Laird, *supra* note 15 ("Some postings have included information for contacting the victim's work supervisor or family.").

65. *See* Citron & Franks, *supra* note 26, at 350–54 (explaining that revenge porn produces serious harms, including offline stalking and attacks, anxiety and depression, loss of employment, and forfeiture of online presence).

66. *See* Franks, *Unwilling Avatars*, *supra* note 45, at 229 ("Women shut down their blogs, avoid websites they formerly frequented, take down social networking profiles, refrain from engaging in online political commentary, and choose not to maintain potentially lucrative or personally rewarding online presences due to cyberspace harassment." (citation omitted)).

an attempt to disassociate themselves from the images. They change jobs, drop out of school, relocate to new cities, or "go into hiding" to avoid threats of sexual abuse and stalking.[67] Along with these external stressors, coping with the anxiety, depression, and self-blame that follows the distribution of nonconsensual pornography proves difficult, and some victims commit suicide.[68]

The harm caused by the unwanted distribution of sexually explicit images reaches both women and men.[69] However, within this Note, many stories and statistics will reflect the effect that revenge porn plays on the lives of female victims.[70] While revenge porn affects both sexes and all sexual orientations,[71] it disproportionately upsets the lives of heterosexual young women as part of a larger class of cyber gender harassment victims.[72]

---

67. *See id.* ("The harms they experience spill over into their offline lives: women have dropped out of school, changed jobs, moved cities, gone into hiding, experienced mental breakdowns, and, in extreme cases, committed suicide." (citation omitted)); Citron, *supra* note 62, at 70 (explaining that by posting identifying information online, the poster places the victim at risk of identity theft, employment discrimination, and stalking).

68. *See* FRANKS, FREQUENTLY ASKED QUESTIONS, *supra* note 46 ("Victims are routinely threatened with sexual assault, stalked, harassed, fired from jobs, and forced to change schools. Some victims have committed suicide."); *FAQ for Victims and Survivors*, WITHOUT MY CONSENT, http://www.withoutmyconsent.org/faq (last visited Nov. 18, 2014) (answering the question, "What are some of the emotional reactions someone whose privacy was violated might have?") (on file with the Washington and Lee Law Review).

69. *See* Citron & Franks, *supra* note 26, at 353 (referring to a study of 1,244 revenge porn victims, of which 90% were female (citation omitted)); Danny Gold, *The Man Who Makes Money Publishing Your Nude Pics*, THE AWL (Nov. 10, 2011), http://www.theawl.com/2011/11/the-man-who-makes-money-publishing-your-nude-pics (last visited Nov. 18, 2014) ("Unlike many co-ed sites out there, Is Anybody Up? features just as many men as women, if not more.") (on file with the Washington and Lee Law Review).

70. *See, e.g.*, Fletcher, *supra* note 1 (detailing the story of Hollie Toups, a revenge porn victim).

71. *See* Bambauer, *Exposed*, *supra* note 30, at 2027–28 (citing surveys that report victims of revenge porn as both heterosexual and LGBT individuals); Franks, *Unwilling Avatars*, *supra* note 45, at 227–28 (noting that while other groups are affected by cyber harassment, special attention should be given to the gendered dimension of online harassment).

72. *See* Franks, *Unwilling Avatars*, *supra* note 45, at 227–28 (mentioning revenge porn within the larger context of cyber harassment).

Most revenge porn victims are young females,[73] and young women are more frequently and severely affected by cyber harassment.[74] Unfortunately, both male and female victims find inadequate remedies in existing legal options and continue to suffer the harms of nonconsensual pornography with little hope of recovery.[75]

III. A Revenge Porn Victim's Existing Legal Options

As states begin to consider specific legislation to battle the growth of nonconsensual pornography, they face criticism from those who believe the answer lies in existing copyright, tort, and criminal law.[76] However, finding relief in existing law often proves difficult. Law enforcement and legal services may blame the victim or dismiss the claims as insignificant.[77] When legal options exist, they prove time-consuming and expensive, and lengthy civil trials lead to extended publicity for an individual already experiencing intense public humiliation.[78] Additionally, while a trial may result in injunctive relief or monetary damages, the images usually remain online.[79] The following subparts

---

73. *See, e.g.*, Franks, A Working Paper, *supra* note 14, at 4 (indicating that the majority of revenge porn victims are women and girls); Laird, *supra* note 15 (noting that revenge porn victims "skew female and young" and that all those who have stepped forward to pursue litigation are female).

74. *See, e.g.*, Franks, *Unwilling Avatars*, *supra* note 45, at 227 ("Cyber harassment affects women disproportionately, both in terms of frequency and in terms of impact.").

75. *See infra* Part III (discussing the inadequacy of existing legal options).

76. *See* Citron & Franks, *supra* note 26, at 357 ("Some commentators oppose regulatory proposals based on the argument that existing civil remedies can ably address revenge porn." (citation omitted)).

77. *See* Levendowski, *supra* note 30, at 425 (noting that victims' claims are "often met with apathy from local police").

78. *See, e.g.*, Jones v. Dirty World Entm't Recordings, LLC, 775 F.3d 398, 404 (6th Cir. 2014) (explaining that the victim's initial lawsuit "sparked national media attention, which precipitated further postings"); Citron & Franks, *supra* note 26, at 357–79 (explaining why existing tort law proves problematic for victims of revenge porn).

79. *See* Citron & Franks, *supra* note 26, at 358–59 ("The removal of images is the outcome that most victims desire above all else, and civil litigation may be unable to make that happen."); Levendowski, *supra* note 30, at 425 (explaining

examine various areas of the law in which a victim may attempt to find relief, as well as explain the shortcomings of each.

A. Copyright Law

Because victims seek removal of all of their images, not just monetary damages or injunctive relief,[80] scholars suggest turning to copyright law.[81] Victims own the copyright to self-authored images, or "selfies," regardless of their intention to share them.[82] Because more than 80% of revenge porn images are self-authored images,[83] these victims may demand removal of the sexually explicit images under § 512 of the Digital Millennium Copyright Act (DMCA).[84] Essentially, the DMCA states that a website loses its "safe harbor" immunity when it receives actual knowledge of infringing materials and fails to act.[85] Under the Act's takedown

---

that victims usually desire removal of the images, not just the injunctive relief or monetary damages that follow civil suits).

80. *See, e.g.*, Levendowski, *supra* note 30, at 425 (explaining that victims want the images removed as quickly as possible).

81. *See, e.g.*, *id.* at 439–46 (explaining why copyright law may protect the majority of revenge porn victims without reworking existing law, abridging free speech, or affecting § 230 immunity); Bambauer, *Beating Revenge Porn with Copyright*, *supra* note 8 (suggesting that revenge porn victims turn to § 512 of the DMCA and explaining possible objections to this solution).

82. *See* 17 U.S.C. § 201(a) (2012) ("Copyright in a work protected under this title vests initially in the author or authors of the work."); Levendowski *supra* note 30, at 443 (noting that a victim need not register the image or hire a lawyer to file a takedown notice (citation omitted)).

83. *See* Levendowski, *supra* note 30, at 426 (referring to a survey of 864 revenge porn victims that revealed that more than 80% of revenge porn images are self-authored images).

84. *See* 17 U.S.C. § 512 (limiting the liability of ISPs that remove or block infringing material upon receipt of actual knowledge or awareness).

85. *See id.* § 512(c)(1) (explaining that a service provider is not liable for copyright infringement if it does not have actual knowledge or if it acts to remove or block the material after receiving such knowledge). Courts have interpreted "actual knowledge" to mean "knowledge of specific and identifiable infringements" rather than general knowledge of infringing activity. *See, e.g.*, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 30–32 (2d Cir. 2012) (relying on the language and basic operation of § 512 to support its finding that the law requires actual knowledge of infringing material). A site may also lose its safe-harbor immunity if it receives financial benefits from the infringing material because it then has the "right and ability to control such activity." 17 U.S.C.

notification procedure, a website may gain such "actual knowledge" when victims of copyright infringement notify the website.[86] If the website removes the infringing image upon such notification, it retains its DMCA immunity. This requirement forces websites either to remove infringing material or to face liability for the copyright infringement,[87] an area of law not covered by § 230 immunity.[88] This solution provides victims of copyright infringement with an efficient and effective way to remove the illicit material.[89]

While the DMCA may aid those with self-authored images, other revenge porn victims find copyright claims challenging and sometimes useless. For example, victims pursuing a potential copyright infringement claim face the serious challenge of proving ownership of the images.[90] Under the DMCA, the claimant must certify that he or she is authorized to act on behalf of the owner of an exclusive right and must do so under penalty of perjury.[91] If the individual captured the image, the claim stands.[92] However, for the nearly 20% of revenge porn victims

---

§ 512(c)(1)(B).

86. *See* 17 U.S.C. § 512(c)(3)(A) (listing elements of notification).

87. *See id.* § 512(c)(1)(C) (explaining that a service provider is not liable for copyright infringement if it receives notification and "responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity").

88. *See* 47 U.S.C. § 230(e) (2012) (noting that this law has no effect on criminal law, intellectual property law, state law, or communications privacy laws); Levendowski, *supra* note 30, at 428 ("ISPs are not required to monitor or proactively remove user-generated content, but § 230 immunity does not extend to violations of child pornography, obscenity, or copyright law." (citations omitted)).

89. *See, e.g.*, *supra* Part III.A (explaining the DMCA's ability to provide prompt relief for some victims of revenge porn).

90. *See* Bambauer, *Beating Revenge Porn with Copyright*, *supra* note 8 (noting that two obstacles may exist for revenge porn victims seeking § 512 relief: not owning the image and certifying under penalty of perjury that they are authorized to act on behalf of the copyright owner).

91. *See* 17 U.S.C. § 512(c)(3)(A)(i) (listing a "physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed" as an element of notification).

92. *See* Levendowski, *supra* note 30, at 339–42 (concluding that copyright solutions may prove helpful to revenge porn victims who self-authored the images).

whose images were captured by their ex-partner or another, authorship proves a nearly impossible hurdle to overcome.[93] Even when a victim proves authorship, a copyright infringement claim may simply be ignored, leading to a costly and time-consuming trial.[94]

Even revenge porn victims able to act under § 512 may encounter obstacles. For example, copyrighted images removed from one revenge porn website may begin appearing on other similar sites, or users may post more sexually explicit images to the original site in retaliation.[95] For victims seeking to regain their privacy, this additional exposure must be considered before pursuing § 512 takedown notices.[96] Additionally, takedown notices to international ISPs may prove ineffective; the ISP may simply refuse to comply with United States law.[97] Investigations into these servers are costly and may only attract more unwanted publicity for victims.[98] Ultimately, § 512 takedown notifications help some revenge porn victims achieve removal but leave many victims without this desired remedy.

---

93. *See id.* at 439–40 (explaining that copyright law provides a solution to those with self-authored images). Some scholars propose a solution under the theory of "joint authorship," though this remains largely untested. *See* 17 U.S.C. § 201(a) (2012) ("The authors of a joint work are co-owners of copyright in the work."); Bambauer, *Beating Revenge Porn with Copyright*, *supra* note 8 (proposing that revenge porn victims may claim joint authorship of revenge porn images because the victim is the subject and the subject holds expressive value in these particular images).

94. *See* Citron & Franks, *supra* note 26, at 360 (noting that many revenge porn websites ignore takedown notices because they know victims cannot afford to hire an attorney).

95. *See* Levendowski, *supra* note 30, at 444 (explaining why takedown notifications may prove problematic).

96. *See id.* ("By issuing a takedown notice—which requires the disclosure of personal information—victims may inadvertently draw *more* attention to the images as the website might create additional posts about victims who request takedowns or encourage users to re-post victims' images onto other websites." (citation omitted)).

97. *See id.* (noting that sites with servers abroad may refuse to follow the law or ignore the takedown requests (citation omitted)).

98. *See id.* ("For victims who are able to afford a lawyer, filing a subpoena seeking the disclosure of servers' locations could potentially attract attention to the images at issue.").

B. Tort Law

In 2012, a Colorado court awarded injunctive relief and $155,000 in damages to a revenge porn victim for intentional infliction of emotional distress and public disclosure of private facts.[99] The woman's ex-boyfriend posted sexually explicit images of her to his blog and other websites with false statements regarding their relationship and her marriage, and he repeatedly e-mailed more images to both the victim and her husband.[100] He created false social media accounts and distributed the images to third parties, who further distributed and publicized the photographs.[101] The court ultimately granted monetary damages and injunctive relief, finding that the poster intended "to destroy Plaintiffs' marriage, to cause Plaintiffs' emotional distress, to harass them, and to stalk them."[102]

Like the Colorado woman, other revenge porn victims may pursue a civil suit for a variety of tort actions.[103] For example, a victim may file an intentional infliction of emotional distress suit if he or she shows that the poster engaged in "extreme and outrageous conduct" that "intentionally or recklessly cause[d] severe emotional harm."[104] A poster—having intentionally posted such an image to a website well-known for dealing in degradation—intentionally, or at least recklessly, inflicts emotional distress onto the victim.[105] However, case law requires

---

99. *See* Doe v. Hofstetter, No. 11-cv-02209-DME-MJW, 2012 WL 3398316, at *1–2 (D. Colo. Aug. 14, 2012) (ordering monetary damages and injunctive relief).

100. *See* Doe v. Hofstetter, No. 11-cv-02209-DME-MJW, 2012 WL 2319052, at *2–4 (D. Colo. June 13, 2012) (listing the defendant's activities, which included contacting the plaintiff, sending her photographs, and publishing false statements about her).

101. *See id.* at *3 (noting that the defendant created a false Twitter account impersonating the plaintiff and communicated to third parties).

102. *Id.*

103. *See* Levendowski, *supra* note 30, at 425 (noting that victims may attempt to pursue stalking, harassment, and invasion-of-privacy suits).

104. *See* RESTATEMENT (THIRD) OF TORTS: PHYS. & EMOT. HARM § 46 (2012) ("An actor who by extreme and outrageous conduct intentionally or recklessly causes severe emotional harm to another is subject to liability for that emotional harm and, if the emotional harm causes bodily harm, also for the bodily harm.").

105. *See supra* notes 47–48 and accompanying text (explaining that posters

that victims suffer a "severely disabling emotional response" or "unendurable" distress.[106] For example, a 2002 Fifth Circuit case held that persistent sexual and physical harassment resulting in anger, humiliation, and embarrassment failed to meet this threshold requirement.[107] Victims of revenge porn, therefore, may struggle to prove that their own humiliation qualifies as severe emotional harm under the law.[108]

A variety of privacy torts may also prove inapplicable. For example, a victim claiming invasion of privacy[109] generally must show a "reasonable expectation of privacy" in the images.[110] This proves challenging when victims voluntarily shared the photographs with romantic partners; society often criticizes the revenge porn victim for her cooperation in the initial distribution, and courts may assume the victim intended extensive permission to distribute the photos.[111] However, allowing one individual to

---

often distribute revenge porn images in an attempt to seek "revenge" on their ex-partners).

106. *See* Smith v. Amedisys Inc., 298 F.3d 434, 450 (5th Cir. 2002) (explaining that the distress must be "unendurable" and victims of sexual harassment who felt angry, embarrassed, disgusted, humiliated, horrified, and repulsed failed to satisfy the threshold required); Harris v. Jones, 380 A.2d 611, 616 (Md. 1977) (finding that plaintiff failed to show that "he suffered a severely disabling emotional response to the defendant's conduct"); RESTATEMENT (THIRD) OF TORTS: PHYS. & EMOT. HARM § 46 cmt. j (explaining that the emotional harm suffered must be severe, such that no reasonable person would be expected to tolerate it).

107. *See Smith*, 298 F.3d at 449 (noting that victims of sexual harassment who felt angry, embarrassed, disgusted, humiliated, horrified, and repulsed failed to satisfy the threshold required of "unendurable duress").

108. *Cf. infra* Part III.D (explaining why the California anti-revenge-porn law's requirements of intent to harm and proof of harm may be difficult to overcome).

109. *See* RESTATEMENT (SECOND) OF TORTS § 652B–D (1965) (defining various invasion-of-privacy torts).

110. *See* Levendowski, *supra* note 30, at 436–37 (noting that invasion-of-privacy suits rarely prove useful for victims of revenge porn because victims must demonstrate a "reasonable expectation of privacy" in the images (quoting Kristin M. Beasley, *Up-Skirt and Other Dirt: Why Cell Phone Cameras and Other Technologies Require a New Approach to Protecting Personal Privacy in Public Places*, 31 S. ILL. U. L.J. 69, 93 (2006))).

111. *See* Citron & Franks, *supra* note 26, at 348 (explaining the misguided belief "that a woman's consensual sharing of sexually explicit photos with a trusted confidant should be taken as wide-ranging permission to share them

view your photograph in the context of a romantic relationship does not permit that individual or others to distribute or view the image without explicit permission.[112] Unfortunately, breaking down societal constructions of consent and victim-blaming may be difficult for most revenge porn victims.[113]

Practical concerns also render the majority of civil claims "more theoretical than real."[114] For example, many victims cannot afford to hire an attorney or refuse to endure additional unwanted publicity.[115] On other occasions, civil suits fail because the poster's identity remains anonymous.[116] When civil suits prove successful, as they did for the young woman in Colorado, monetary damages may be difficult to collect or may be unsatisfactory when the victim seeks removal of the images.[117] Ultimately, victims find themselves abandoning these civil remedies and turning to other areas of the law.

C. Criminal Law

With practical concerns limiting the effect of tort law, victims should be able to turn to criminal law for protection. In theory, criminal law provides a variety of desirable benefits. For example, when a poster is criminally punished for an illicit post, the legal system acknowledges the seriousness of the harm caused by revenge porn.[118] It also deters perpetrators who might

---

with the public" (citation omitted)).

112. *See id.* (explaining that consent is context-specific).

113. *Id.*

114. *See id.* at 357 ("Civil law can offer modest deterrence and remedy, but practical concerns often render them more theoretical than real.").

115. *See id.* at 358–59 (explaining that the problem with civil suits lies in victims' inability to hire an attorney or their reluctance to proceed under their real names).

116. *Cf.* Richards, *infra* note 229, at 179 (explaining the problems that often follow anonymous online posts).

117. *See* Citron & Franks, *supra* note 26, at 358 (noting that it may be difficult for victims to recover damages and that even an award of damages "is no assurance that websites will comply with requests to take down the images").

118. *See id.* at 361–62 ("Criminal law is essential to send the clear message to potential perpetrators that nonconsensual pornography inflicts grave privacy and autonomy harms that have real consequences and penalties." (citation

dismiss the threat of a civil suit yet fear the serious and permanent consequences of criminal conviction.[119] In addition, § 230 limits immunity when federal criminal law applies, allowing victims to attack the website operators.[120] Unfortunately, prosecutors struggle to apply existing law to the unique and relatively new concept of revenge porn, leaving victims with little hope of finding redress in criminal law.[121]

Revenge porn distribution often involves a variety of criminal behaviors, such as hacking, extortion, and the distribution of child pornography.[122] Unfortunately, relevant criminal law applies in very limited circumstances.[123] For example, all fifty states impose criminal sanctions for various computer crimes, including computer trespass and unauthorized use of a computer.[124] If a poster hacked into a victim's computer or other electronic device and removed photographs or videos, the victim may have a valid claim under criminal law.[125] However, the majority of revenge porn images result from jilted ex-partners who originally obtained the photographs and videos with consent; these victims will find no recourse in hacking laws.[126] Federal

---

omitted)).

119. *See id.* at 361 (explaining that a criminal conviction may deter some perpetrators more than a civil suit).

120. *See* 47 U.S.C. § 230(e) (2012) (noting that § 230 has no effect on "any other Federal criminal statute").

121. *See* Citron & Franks, *supra* note 26, at 365–70 (explaining the limitations of current criminal law).

122. *See id.* (noting various criminal acts that are associated with revenge porn and explaining why existing criminal law fails to address these issues).

123. *See id.* (explaining why existing criminal laws fail to cover revenge porn).

124. *See Computer Crime Statutes*, http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx (last updated June 27, 2014) (last visited Nov. 18, 2014) (listing computer crime statutes for all fifty states) (on file with the Washington and Lee Law Review).

125. *See, e.g.*, CAL. PENAL CODE § 502(c)(2) (West 2013), *amended by* 2014 Cal. Legis. Serv. Ch. 379 (A.B. 1649) (West) (prohibiting the unauthorized taking, copying, or use of data from a computer, computer system, or computer network).

126. *See supra* note 47 and accompanying text (noting that most revenge porn results from jilted ex-partners).

extortion laws, which extend beyond the reach of § 230 immunity, also apply in only a limited number of revenge porn cases.[127] These laws apply when websites charge significant fees to remove the photographs, but some sites do not charge fees and simply refuse to remove the images; victims of these sites will find no relief in extortion claims.[128] Similarly, child pornography laws may prove helpful, but they apply to a limited number of victims.[129] These laws aid victims in removing images, and even shutting down websites, when the subject was under eighteen years of age at the time the photograph was taken.[130]

Other criminal laws prove ineffective for nearly all revenge porn victims. For example, state and federal cyber harassment statutes require the perpetrator to engage in a "course of conduct" that places the victim in reasonable fear of bodily harm or that could reasonably be expected to cause "substantial" emotional harm.[131] Revenge porn may be reposted again and again by third parties, resulting in serious and irreparable harm; however, the poster only uploaded the original post.[132] Because the poster only uploads the image once, or maybe a handful of times, it is unlikely that it amounts to a "course of conduct" necessary to

---

127. *See, e.g.*, *"Revenge Porn" Website Gets Calif. Man Charged with Extortion*, CBS (Dec. 11, 2013, 4:49 PM), http://www.cbsnews.com/news/calif-man-charged-with-extortion-through-revenge-porn-website/ (last visited Nov. 18, 2014) (reporting the arrest of the operator of UGotPosted.com, who charged victims $250–$350 to remove their images from his website) (on file with the Washington and Lee Law Review).

128. *But see* Citron & Franks, *supra* note 26, at 368 (noting that federal prosecutors have expressed interest in pursuing extortion claims against revenge porn website operators).

129. *See, e.g.*, 18 U.S.C. § 2252 (2012) (prohibiting certain acts relating to child pornography, including possession, distribution, and receipt).

130. *See* Fletcher, *supra* note 1 (noting that Hollie Toups's private investigators shut down the website Texxxan.com on child pornography charges).

131. *See, e.g.*, 18 U.S.C. § 2261A (requiring that the perpetrator's behavior place a person in reasonable fear of death or injury or cause, or attempt to cause, "substantial emotional distress").

132. *See* Levendowski, *supra* note 30, at 432 ("The harm caused by revenge porn . . . is accomplished through the one-off act of uploading a sexually explicit image.").

violate existing cyber harassment statutes.[133] Unable to satisfy these elements, victims find little relief in criminal law.

D. Enacted and Proposed State Legislation

Though existing law may prove ineffective to combat the distribution of nonconsensual pornography, some states are attempting to create specific anti-revenge-porn legislation.[134] State criminal law does not affect the § 230 immunity of interactive computer services,[135] but such legislation undoubtedly holds the potential to deter would-be posters and punish current offenders.[136] Unfortunately, states considering anti-revenge-porn legislation face serious challenges as they struggle to achieve these goals and still respect the constitutionally guaranteed rights of posters.[137]

For example, California recently passed a law targeting the distribution of nonconsensual pornography.[138] The California law makes it a misdemeanor to photograph or record the "intimate body part or parts" of an identifiable individual and then distribute those images with the intent to cause, and causing, serious emotional distress.[139] Victims are hindered, however, by

---

133. *See id.* (noting that victims will often fail to prove a "course of conduct" because harms result from third parties' reposting and redistribution of the images rather than through repetitive and ongoing acts by the original poster).

134. *See supra* note 27 and accompanying text (listing various state anti-revenge-porn legislation).

135. *See* 47 U.S.C. § 230(e)(1) (2012) (noting that § 230 has no effect on federal criminal statutes).

136. *See* Citron & Franks, *supra* note 26, at 361 ("A criminal law solution is essential to deter judgment-proof perpetrators.").

137. *See, e.g.*, *infra* note 141 and accompanying text (noting that the American Civil Liberties Union and Electronic Frontier Foundation attacked California's proposed anti-revenge-porn bill).

138. *See* CAL. PENAL CODE § 647(j)(4)(A) (West 2013), *amended by* 2014 Cal. Legis. Serv. Ch. 71 (S.B. 1304) (West) (prohibiting the recording and subsequent distribution of images of intimate body parts of another identifiable individual when the parties understand that the images are to remain private and the individual has not consented to distribution).

139. *See id.*

> Any person who photographs or records by any means the image of the intimate body part or parts of another identifiable person, under

the requirement that they prove not only "serious emotional distress" but also the posters' intent to cause such emotional harm.[140] This requirement developed after serious criticism from the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation (EFF).[141] These organizations expressed concern that anti-revenge-porn laws could be interpreted too broadly and may allow states to criminalize a wide array of speech, including distribution of photographs carrying a political message.[142] As one activist noted, "We generally don't think that finding more ways to put people in prison for speech is a good thing."[143]

In response to these criticisms, California narrowed the scope of its law by adding the intent and proof of harm requirements.[144] Some argue that the law now passes constitutional muster because it targets a type of speech that receives less First Amendment protection.[145] When speech falls into certain

---

> circumstances where the parties agree or understand that the image shall remain private, and the person subsequently distributes the image taken, with the intent to cause serious emotional distress, and the depicted person suffers serious emotional distress.

140. *See id.* (including the requirement that the perpetrator "subsequently distributes the image taken, with the intent to cause serious emotional distress, and the depicted person suffers serious emotional distress").

141. *See* Anne Flaherty, *Revenge Porn Victims Pursue New Laws, But ACLU Urges Caution*, BOS. GLOBE (Nov. 16, 2013), http://www.bostonglobe.com/news/nation/2013/11/16/revenge-porn-victims-press-for-new-laws/cXQNeLzOcy7oSDTUh3W5fK/story.html (last visited Nov. 18, 2014) (explaining that members of the ACLU and EFF believe these laws risk becoming an overly broad criminalization of speech) (on file with the Washington and Lee Law Review).

142. *See id.* ("The [Maryland] bill would exclude images deemed to have 'public importance'—an exemption carved out in response to critics who say such laws would criminalize the publishing of explicit photos by journalists.").

143. *Id.*

144. *See id.* (noting that the ACLU's California office worked to dilute the California anti-revenge-porn law).

145. *See, e.g.*, Citron & Franks, *supra* note 26, at 374–86 (addressing the First Amendment concerns associated with anti-revenge-porn legislation); *id.* at 387 (providing recommendations for future state legislation and suggesting similar intent requirements to avoid over-breadth issues). Courts have not yet ruled on the constitutionality of anti-revenge-porn legislation, and some scholars suggest that it will prove unconstitutional. *See, e.g.*, Bambauer, *Exposed*, *supra* note 30, at 54–55 (arguing that revenge porn is not "an unprotected expression that the government may regulate at will").

categories such as obscenity, child pornography, or true threats, it proves unworthy of full First Amendment protections because it is not an "essential part of any exposition of ideas and [is] of such slight social value that any benefit that may be derived from [it is] clearly outweighed by the social interest in order and morality."[146] Harmful revenge porn images may therefore be regulated.[147] However, newsworthy images or those distributed as matters of public concern retain their First Amendment protection because they are distributed with the intent to inform the public rather than harm an individual,[148] and such public issues should be freely disseminated.[149] Unfortunately, these restraints significantly narrow the protection available to revenge porn victims, who must now prove intent to cause emotional distress and actual emotional harm.[150]

Other states attempting to provide relief to revenge porn victims are hindered by these same constitutional concerns. For example, Florida, which abandoned an anti-revenge-porn law in 2013 due to free speech concerns,[151] attempted to make it a felony

---

146. FCC v. Pacifica Found., 438 U.S. 726, 746 (1978) (quoting Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942)); *see also* Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 758 (1985) ("We have long recognized that not all speech is of equal First Amendment importance.").

147. *See* Citron & Franks, *supra* note 26, at 384–85 (agreeing with scholar Eugene Volokh that nonconsensual pornography falls within the unprotected category of obscenity).

148. *Cf. id.* at 388 (recommending exemptions for newsworthy publications in an effort to avoid First Amendment concerns).

149. *See, e.g.*, N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279–80 (1964) (requiring public officials to prove "actual malice" for defamatory statements). In *Sullivan*, the Court noted, "[W]e consider this case against the background of a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials." *Id.* at 270.

150. *See, e.g.*, Eric Goldman, *California's New Law Shows It's Not Easy to Regulate Revenge Porn*, FORBES (Oct. 8, 2013, 12:03 PM), http://www.forbes.com/sites/ericgoldman/2013/10/08/californias-new-law-shows-its-not-easy-to-regulate-revenge-porn/ (last visited Nov. 18, 2014) (explaining why "insufficient intent to cause emotional distress" may bar some victims' claims) (on file with the Washington and Lee Law Review).

151. *See* H.R. 787, 115th Reg. Sess. (Fla. 2013) (prohibiting the knowing use of a computer or other similar device to transmit or post nude images of another without first obtaining consent from the photographed individual); Heather

to disclose sexually explicit images of a person with identifying information, without that person's consent.[152] However, not unlike California's law, the Florida law required intent to harass, and it died in committee in May 2014.[153] Maryland's anti-revenge-porn law, passed in March 2014, similarly requires intent to cause "serious emotional distress."[154] Conversely, Wisconsin's anti-revenge-porn law does not include an intent requirement.[155] The Wisconsin legislature did, however, indicate an attempt to avoid First Amendment concerns when it added a provision regarding the distribution of newsworthy publications.[156] By providing an exception for material that is "newsworthy or of public importance," Wisconsin attempts to provide an affirmative defense to those postings distributed for their informative value and not for harm.[157] With the passage of these laws—constrained by the Constitution and limited by intent requirements—it becomes clear that even specific anti-revenge-porn legislation fails to provide adequate protections for victims.

Kelly, *New California "Revenge Porn" Law May Miss Some Victims*, CNN (Oct. 3, 2013, 6:32 AM), http://www.cnn.com/2013/10/03/tech/web/revenge-porn-law-california/ (last visited Nov. 18, 2014) ("Florida was considering a revenge porn law but scrapped it following First Amendment concerns.") (on file with the Washington and Lee Law Review).

152. *See* H.R. 475, 116th Reg. Sess. (Fla. 2014) (prohibiting the intentional nonconsensual disclosure of a sexually explicit image of an identifiable individual for the purposes of harassment).

153. *See id.* (prohibiting the disclosure of "a sexually explicit image of an identifiable person with the intent to harass such person").

154. *See* H.R. 43, 434th Gen. Assemb. (Md. 2014) (to be codified at MD. CODE, CRIM. LAW § 3-809) ("A person may not knowingly disclose [an image] of another person whose intimate parts are exposed or who is engaged in an act of sexual contact, without the consent of the other person and with the intent to cause serious emotional distress.").

155. *See* WIS. STAT. ANN. § 942.09 (West 2014) (prohibiting the distribution of sexually explicit images without the consent of the photographed individual, but failing to include an intent requirement).

156. *See id.* § 942.09(3)(b)(3) (explaining that this law does not apply to "a person who posts or publishes a private representation that is newsworthy or of public importance").

157. *Cf.* Citron & Franks, *supra* note 26, at 388 (recommending future legislation include clear exemptions for matters of public importance to avoid over-breadth).

IV. The Challenge of Combating Revenge Porn: § 230 Immunity

Considering the limited legal options available to revenge porn victims, it may seem logical to pursue the website operator, rather than the poster, to provide victims with a way to remove the harmful images. Unfortunately, § 230 of the CDA[158] provides broad civil immunity for website operators and ISPs, preventing such suits.[159] This Part explains the law,[160] as well as the development of traditional § 230 jurisprudence, which interprets § 230 immunity in broad terms.[161] It also explores emerging case law that attempts to limit this immunity.[162]

A. The Communications Decency Act

The CDA was passed on February 1, 1996, as an amendment to the Telecommunications Act of 1996.[163] Section 230 states, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[164] An interactive computer service includes "any information service, system, or access software that provides or enables computer access by multiple users to a computer server."[165] This definition embraces any website or online service, such as a website's web-hosting

158. 47 U.S.C. § 230 (2012).

159. *See id.* § 230(c)(1) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

160. *See infra* Part IV.A (explaining the development of § 230).

161. *See infra* Part IV.B (discussing traditional interpretations of § 230 immunity).

162. *See infra* Part IV.C (explaining recent cases that move away from traditional interpretations of § 230 immunity).

163. *See* Joel R. Reidenberg et al., *Section 230 of the Communications Decency Act: A Survey of the Legal Literature and Reform Proposals* 4 (Fordham Law Legal Studies Research Paper No. 2046230, 2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2046230 (explaining the legislative history of the CDA).

164. § 230(c)(1) (2012).

165. *See id.* § 230(f)(2) (defining "interactive computer service").

company.[166] These websites and online services retain civil immunity so long as they do not become "information content providers," or "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[167] Essentially, the services cannot create or develop the unlawful material; however, failing to remove or edit the material after notice or revising such material often fails to qualify the ISP as an "information content provider."[168] Instead, the original content provider, or poster, of the information remains solely liable because that individual is responsible, in whole or part, for creating the material.[169]

While the CDA grew out of concern for pornography on the Internet,[170] § 230 addressed confusion and concerns within the Internet industry.[171] Under the common-law approach, ISPs that used editorial control and judgment to regulate defamatory postings were subject to higher levels of liability than ISPs that

---

166. *See, e.g.*, Klayman v. Zuckerberg, 910 F. Supp. 2d 314, 318 (D.D.C. 2012) (explaining that Facebook, a social media website, provided and enabled access to a computer server to multiple users, and therefore qualified as a an interactive computer service); Reidenberg, *supra* note 163, at 1 (defining the term "interactive computer service" and noting that it has "been broadly interpreted to include any website or online service"). Even Internet providers like Comcast have been labeled "interactive computer services" and therefore qualify for § 230 immunity. *See, e.g.*, e360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605, 609–10 (N.D. Ill. 2008) (providing § 230 immunity to Comcast for its "good Samaritan" blocking and filtering of solicitous e-mails).

167. *See* 47 U.S.C. § 230(f)(3) (defining "information content provider").

168. *See infra* Part IV.B (explaining traditional interpretations of § 230 immunity). *But see infra* Part IV.C (describing a movement away from traditional interpretations of § 230 immunity that imposes liability for certain levels of editorial control).

169. *See, e.g.*, Sarah Duran, *Hear No Evil, See No Evil, Spread No Evil: Creating a Unified Legislative Approach to Internet Service Provider Immunity*, 12 U. BALT. INTELL. PROP. L.J. 115, 119–20 (2004) ("[The CDA] states that a provider or user of an interactive computer service cannot be treated as a publisher or speaker of information when someone else is providing the speech; the liability goes solely to the content provider . . . .").

170. *See* Reidenberg, *supra* note 163, at 6 (noting that original drafts of the CDA were created with "the primary goal of protecting children from pornography on the Internet").

171. *See id.* at 4–6 (explaining the common-law approach to ISP immunity before § 230 and the concern it caused among the computer services industry).

followed a more "hands-off" approach and simply failed to remove defamatory material after notification.[172] This unfair standard essentially punished self-regulating ISPs, while rewarding "hands-off" ISPs with lower levels of liability.[173] To resolve this issue, Congress created § 230.[174] This provision provides civil immunity for ISPs and operators from the actions of third-party posters, even when the ISP or operator uses editorial control over the illicit material.[175]

B. Traditional Interpretations of § 230 Immunity

Since the enactment of § 230 in 1996, many courts have interpreted the provision to provide a broad level of immunity to interactive computer services.[176] In 1997, only one year after the

---

172. *See* Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *3 (N.Y. Sup. Ct. May 24, 1995) (holding the defendant computer service to the higher standard of "publisher liability" because it screened and removed messages on its site); Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 139–41 (S.D.N.Y. 1991) (applying "distributor liability" to the defendant computer network but finding that the defendant did not have knowledge of the allegedly defamatory statements on its sites and could not be held liable for those statements); Reidenberg, *supra* note 163, at 4–6 (explaining the common-law approach of applying "distributor liability" for failure to remove after obtaining knowledge and "publisher liability" for repeatedly republishing the material).

173. *See* Reidenberg, *supra* note 163, at 5–6 (explaining that the two standards of liability led members of the computer services industry to believe that ISPs would be discouraged from screening content because it would expose them to excessive liability).

174. *See id.* ("The irreconcilability of a higher standard of liability for publisher-ISPs that attempted to monitor for offensive content compared to distributor-ISPs, those who 'let anything go,' prompted legislative reform.").

175. *See* 47 U.S.C. § 230(c)(1) (2012) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."); *id.* § 230(c)(2)(A) (explaining that computer services will not be held liable for "actions taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected").

176. *See, e.g.*, Chi. Lawyer's Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 669–72 (7th Cir. 2008) (refusing to limit the § 230 immunity of the defendant website when third-party postings on the site

CDA's enactment, the U.S. Court of Appeals for the Fourth Circuit addressed the issue in *Zeran v. America Online, Inc.*[177] In *Zeran*, an anonymous AOL user posted advertisements to the website's bulletin boards, promoting the sale of shirts with offensive slogans relating to the Oklahoma City federal building bombing of 1995.[178] The user listed Kenneth Zeran's home telephone number and directed interested users to contact him for purchase information.[179] Zeran then received numerous phone calls, including "angry and derogatory" messages and death threats.[180] Though Zeran notified AOL and received assurances of removal, the anonymous postings continued, and Zeran finally sued the website.[181] Ultimately, the Fourth Circuit found that AOL held § 230 immunity despite its notice of the illicit material and its subsequent failure to act.[182] In its decision, the court noted that § 230 provided immunity from both the republishing of illicit material and the failure to remove illicit material after notification.[183]

---

violated the Fair Housing Act); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1125 (9th Cir. 2003) (providing broad immunity to a matchmaking website that generated user profiles based on user answers to a questionnaire created by the website); Zeran v. Am. Online, Inc., 129 F.3d 327, 330–34 (4th Cir. 1997) (refusing to limit the immunity of the defendant website even though it received notice of the offending material and substantially delayed removal of the material); Blumenthal v. Drudge, 992 F. Supp. 44, 51–53 (D.D.C. 1998) (allowing AOL to retain its § 230 immunity despite defamatory statements made in an online gossip column, the author of which had a licensing agreement with AOL allowing it to remove and edit stories).

177. *See* 129 F.3d 327, 330–34 (4th Cir. 1997) (allowing defendant website to retain immunity despite notice and delayed removal of offending material).

178. *See id.* at 329 (explaining the facts behind the plaintiff's action against America Online, Inc.).

179. *See id.* (explaining the facts behind the plaintiff's allegations).

180. *See id.* (noting that the plaintiff received "a high volume of calls, comprised primarily of angry and derogatory messages, but also including death threats"). As the postings continued, Zeran received an "abusive" phone call roughly every two minutes. *Id.*

181. *See id.* (noting that the plaintiff contacted AOL repeatedly, but the anonymous user continued to post additional advertisements).

182. *See id.* at 332 (explaining that AOL is "clearly protected" by § 230 immunity).

183. *See id.* at 331–33 (explaining why § 230 should be read to include both distributor liability and publisher liability).

In reaching this decision, the Fourth Circuit relied heavily on Congress's policy goals in enacting § 230.[184] As the court explained, Congress believed that tort-based lawsuits might threaten free speech in "the new and burgeoning Internet medium."[185] Such tort-based liability would be "simply another form of intrusive government regulation of speech," and Congress wished instead to maintain the "robust nature of Internet communication."[186] Essentially, Congress understood that interactive computer services might limit online speech if forced to continuously screen millions of postings for tortious material.[187] By creating § 230, Congress aimed to remove any such disincentives to self-regulation.[188] Specifically, interactive computer services may use editorial control to regulate offensive material and still retain their § 230 immunity.[189] In theory, this allows these online services to self-police and remove offensive material without fear of civil liability.[190]

Some scholars consider *Zeran* to be the "most significant decision interpreting § 230,"[191] and many courts follow its broad interpretation of § 230 immunity.[192] For example, in *Carafano v.*

---

184. *See id.* at 330–31 (explaining the policy behind § 230).

185. *See id.* at 330 ("Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium.").

186. *See id.* (explaining that Congress enacted § 230 to protect communication on the Internet).

187. *See id.* at 331 ("Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted."); *id.* ("Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.").

188. *See id.* (noting that an important purpose of § 230 was "to encourage service providers to self-regulate the dissemination of offensive material" and explaining that Congress enacted § 230 "to remove the disincentives to self-regulation").

189. *See* 47 U.S.C. § 230(c)(2)(A) (2012) (noting that interactive computer services may not be held liable for good-faith efforts to control access to offensive material).

190. *But see infra* Part V.C (discussing § 230's failure to incentivize self-regulation).

191. *See* Reidenberg, *supra* note 163, at 10 ("*Zeran v. American Online, Inc.* is by far the most significant decision interpreting Section 230.").

192. *See, e.g.*, Chi. Lawyer's Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 669–72 (7th Cir. 2008) (refusing to hold the

Metrosplash.com,[193] the U.S. Court of Appeals for the Ninth Circuit provided broad immunity to a matchmaking website that created a false and defamatory profile of a well-known actress.[194] The information for the profile stemmed from a questionnaire created by the website and answered by an unknown prankster.[195] The sexually explicit language of the questionnaire answers caused the actress to receive numerous calls, voicemails, and e-mails from various men.[196] The actress's manager notified the website but found that only the poster held permission to remove the profile; however, it was eventually blocked and deleted by the website.[197] The Ninth Circuit found that the matchmaking site retained immunity despite its involvement in creating the profile because the harmful information came from the actual poster.[198] Like the Fourth Circuit in *Zeran*, the Ninth Circuit also relied on Congress's policy rationale.[199] With such heavy weight given to these policy goals, the traditional view of § 230 immunity provides broad levels of protection to interactive computer services and severely limits revenge porn victims' ability to gain redress from offending websites.

---

defendant website liable for the notices posted by users); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1125 (9th Cir. 2003) (providing broad immunity to a matchmaking website that created a questionnaire to facilitate profile creations); Blumenthal v. Drudge, 992 F. Supp. 44, 51–53 (D.D.C. 1998) (allowing AOL to retain its § 230 immunity despite its licensing contract that allowed it to remove and edit stories in which defamatory statements were made).

193. 339 F.3d 1119 (9th Cir. 2003).

194. *See id.* at 1125 (concluding that Congress intended websites like the defendant matchmaking site to be afforded immunity from such suits and therefore ruling for the defendant site).

195. *See id.* at 1121 (reciting the facts of the case).

196. *See id.* at 1121–22 (explaining that the plaintiff received numerous sexually explicit calls and messages as a result of the profile).

197. *See id.* at 1122 (explaining the eventual deletion of the profile).

198. *See id.* at 1125 ("Matchmaker did not play a significant role in creating, developing, or 'transforming' the relevant information.").

199. *See id.* at 1123–24 (relying on *Zeran*'s interpretations of Congress's policy goals).

C. The Movement Away from Broad Interpretations of § 230 Immunity

Despite the traditional view of the CDA, emerging case law supports a movement away from broad interpretations of § 230 immunity.[200] *Fair Housing Council of San Fernando Valley v. Roommates.com*[201] was the first case to depart substantially from the broad interpretations of immunity provided by cases such as *Zeran* and *Carafano*.[202] In *Roommates*, website operators created and used a questionnaire to match roommates and required users to answer questions regarding gender, sexual orientation, and family status.[203] The Ninth Circuit found that the website, by creating the offensive material within the questionnaire, became a "developer" of the information, rather than a "passive transmitter."[204] In shifting from traditional applications of § 230, the Ninth Circuit explained that the CDA "was not meant to create a lawless no-man's-land on the Internet."[205]

This movement away from broad immunity is significant, especially considering the Ninth Circuit's ruling five years earlier in *Carafano*.[206] Instead of relying heavily on Congress's stated policy goals, *Roommates* seemed to recognize that some of

---

200. *See, e.g.*, Fair Hous. Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157, 1165 (9th Cir. 2008) (finding that a roommate-matching website became too involved in the illicit conduct when it created and distributed the questionnaire that led to discrimination); Jones v. Dirty World Entm't Recordings, LLC, 840 F. Supp. 2d 1008, 1012 (E.D. Ky. 2012) (finding a website liable for the postings of third parties when the website encouraged the defamatory postings).

201. 521 F.3d 1157 (9th Cir. 2008).

202. *See* Reidenberg, *supra* note 163, at 15 (noting that *Roommates* was the "first major departure" from traditional broad readings of § 230 immunity).

203. *See Roommates*, 521 F.3d at 1161–62 (explaining the Roommates.com profile application process).

204. *See id.* at 1166 ("By requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommate becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information.").

205. *Id.* at 1164.

206. *See supra* Part IV.B (explaining traditional interpretations of § 230 immunity, including *Carafano*).

Congress's rationales may be outdated.[207] For example, Congress created § 230 because it "recognized the threat that tort-based lawsuits pose[d] to freedom of speech in the *new and burgeoning Internet medium*."[208] Essentially, Congress aimed to protect the "free market" of the Internet and thereby allow it to flourish.[209] In 1997, roughly one year after Congress enacted the CDA, about 22.1% of American adults used the Internet[210] and only 18% accessed the Internet at home.[211] Only fifteen years later, in 2012, 74.7% of Americans used the Internet.[212] As the Internet grows stronger, it also grows more pervasive, with 74.8% of Americans accessing the Internet in their homes in 2012.[213] Revenge porn distribution websites profit from this growing medium, making thousands of dollars each month from advertisements or payments for removal of the images.[214] Recognizing this trend, *Roommates* may be correct in challenging Congress's protection of interactive computer services and instead imposing protections for Internet users.

---

207. *See, e.g.*, Duran, *supra* note 169, at 124 ("Although the rationale behind the Act may have made sense when it was passed in 1996, those reasons are no longer convincing.").

208. *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (explaining Congress's policy goals in creating § 230).

209. *See* 47 U.S.C. § 230(b)(2) (2012) (explaining that one policy goal of Congress is "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation").

210. *See* Duran, *supra* note 169, at 124 (referring to U.S. Census reports to indicate the rising trend in Internet use (citation omitted)).

211. U.S. CENSUS BUREAU, COMPUTER AND INTERNET TRENDS IN AMERICA: COMPUTER AND INTERNET USE 1984–2012, 1 (2014) [hereinafter COMPUTER AND INTERNET USE 1984–2012], http://www.census.gov/hhes/computer/files/2012/Computer_Use_Infographic_FINAL.pdf.

212. *Reported Internet Usage for Individuals 3 Years and Older, By Selected Characteristics: 2012*, U.S. CENSUS BUREAU (2014), http://www.census.gov/hhes/computer/publications/2012.html (last visited Nov. 18, 2014) (on file with the Washington and Lee Law Review).

213. *See* COMPUTER AND INTERNET USE 1984–2012, *supra* note 211, at 1 (citing recent changes in "America's relationship with computers").

214. *See* Laird, *supra* note 15 (noting that Hunter Moore claimed to make $30,000 each month from IsAnyoneUp.com and explaining that many more sites profit today from the industry).

Other courts have similarly challenged traditional interpretations of § 230, but with varying degrees of success. Most recently, in *Jones v. Dirty World Entertainment Recordings, LLC*,[215] the U.S. District Court for the Eastern District of Kentucky ruled that § 230 immunity may be forfeited if the website encourages the posting of unlawful materials.[216] In *Jones*, the defendant website invited users to post images and comment about the photographed individuals.[217] This led to a string of photographs and comments about a Cincinnati Bengals cheerleader, who eventually sued for defamation and intentional infliction of emotional distress.[218] The district court held that, by inviting libelous postings that invaded the privacy rights of the plaintiff, the site became a developer and therefore lost its § 230 immunity.[219] The defendants appealed the decision, and the U.S. Court of Appeals for the Sixth Circuit reversed.[220] The Sixth Circuit found that inviting comments and selecting posts for publication failed to transform the website into a developer of harmful material.[221]

While the district court's decision in *Jones* initially suggested a movement away from broad § 230 immunity, the Sixth Circuit's decision turns back to limitless immunity and highlights an important point: not all courts are willing to abandon traditional interpretations of § 230.[222] For example, in *Chicago Lawyer's Committee for Civil Rights Under the Law v. Craigslist*,[223] the

---

215. 840 F. Supp. 2d 1008 (E.D. Ky. 2012).

216. *See id.* at 1011 (explaining that an ISP becomes responsible for the development of material when it "encourages the development of *what is offensive about the content*" (quoting Fair Hous. Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157, 1199 (9th Cir. 2008)).

217. *See id.* at 1009–10 (reciting the facts of the case).

218. *Id.*

219. *See id.* at 1012 (applying *Roommates* to hold the defendant website liable).

220. Jones v. Dirty World Entm't Recordings, LLC, 775 F.3d 398 (6th Cir. 2014).

221. *See id.* at 415–17 (explaining why the website failed to qualify as a developer of information under traditional interpretations of § 230 immunity).

222. *See supra* note 176 and accompanying text (noting several courts that followed the broad interpretation of § 230 immunity).

223. 519 F.3d 666 (7th Cir. 2008).

popular website Craigslist found itself publishing housing advertisements that violated the Fair Housing Act.[224] Craigslist retained immunity because third-party posters, rather than the website operators, created the ads.[225] While the Seventh Circuit noted that § 230 fails to provide a "general prohibition of civil liability," it allows broad civil immunity to websites unless they create or develop the information.[226] Supporting Congress's policy rationale, the Seventh Circuit explained that screening massive amounts of online data for unlawful material would be costly, difficult, and sometimes ineffective.[227]

Despite the shift demonstrated by *Roommates* and despite the district court's interpretations of § 230 in *Jones*, most courts—like the Sixth and Seventh Circuits—continue to rely on Congress's goals of incentivizing self-regulation and protecting the free market of the Internet. Unfortunately, revenge porn and other forms of online abuses continue to spread more rapidly across the Internet, and these victims cannot wait for a more substantial change in § 230 jurisprudence. Instead, legislative action is necessary to reform § 230 and provide relief for victims of nonconsensual pornography and other forms of online harassment.

---

224. *Id.* at 668 (reciting the facts of the case); *see also* Fair Housing Act, 46 U.S.C. § 3604 (2012).

225. *See Chicago Lawyer's Committee*, 519 F.3d at 672 ("[G]iven §230(c)(1) [the plaintiff] cannot sue the messenger just because the message reveals a third-party's plan to engage in unlawful discrimination.").

226. *See id.* at 669 (looking to past Seventh Circuit rulings to explain that "§ 230(c) as a whole cannot be understood as a general prohibition of civil liability for web-site operators and other online content hosts").

227. *See id.* at 668–69 (explaining the difficulty in screening massive amounts of material). Craigslist continues its policy of relying on customer notification instead of pre-screening postings; however, the website added a disclaimer explaining that "[w]hen making any posting on craigslist, [posters] must comply with section 3604(c) of the Federal Fair Housing Act." *Fair Housing Act Information*, CRAIGSLIST, http://www.craigslist.org/about/FHA (last visited Nov. 18, 2014) (on file with the Washington and Lee Law Review).

V. Proposal to Reform § 230 of the Communications Decency Act

To provide relief for victims of nonconsensual pornography, this Note proposes an amendment to § 230 to limit civil immunity of interactive computer services by requiring action upon notification of tortious activity.[228] Legal scholars encourage similar limitations to § 230 immunity in the context of cyberbullying or to create a more unified approach to ISP liability.[229] Such limitations are not unprecedented, as evidenced by § 512 of the DMCA.[230] Section 512's "safe harbor" immunity allows a victim to demand removal of a self-authored image and imposes liability on those ISPs who refuse to remove the copyrighted image.[231] For those victims whose images are not self-authored, this means of removal does not exist because the current CDA provides expansive immunity from the actions of third parties. These websites, therefore, remain free from civil liability despite notification of harmful materials and refusal to remove those images.[232] To resolve this conflict and provide an adequate remedy for victims, Congress should similarly limit the immunity of ISPs under the CDA by adding takedown notification procedures.

---

228. *See infra* Part V.A (detailing the proposed amendment).

229. *See, e.g.*, Bradley A. Areheart, *Regulating Cyberbullies Through Notice-Based Liability*, 41 YALE L.J. POCKET PART 41, 41 (2007) (explaining why the government should implement takedown procedures "to curtail ISP immunity for certain forms of tortious cyberbullying"); Duran, *supra* note 169, at 133–35 (encouraging Congress to adopt a unified approach to regulating ISP liability). Other scholars simply urge that the § 230 is "ripe for reform." *See, e.g.*, Robert D. Richards, *Sex, Lies, and the Internet: Balancing First Amendment Interests, Reputational Harm, and Privacy in the Age of Blogs and Social Networking*, 8 FIRST AMEND. L. REV. 176, 190–97 (2009) (explaining recent developments in § 230 jurisprudence that may indicate future changes to the CDA).

230. *See* 17 U.S.C. § 512(c)(1) (2012) (requiring removal or disabling of infringing material upon notification).

231. *Id.* § 512(c).

232. *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997) (finding that defendant computer service retained § 230 immunity despite notification of harmful material and failure to remove or block the material).

A. Proposed Amendment to Limit § 230 Immunity

To create an effective and efficient takedown notification procedure, Congress should look to the DMCA's procedures and attempt to create a similar amendment within the CDA. However, while the DMCA allows for removal upon notification and provides a foundation for this proposal, the amendment should not parallel the DMCA in every sense. For example, § 512(c)(1) of the DMCA holds ISPs liable once they receive actual knowledge of infringing material and fail to respond in accordance with the act.[233] However, requiring action upon any knowledge—even knowledge obtained through self-policing—of tortious activity may discourage self-regulation, a stated policy goal of § 230.[234] To avoid this issue, the amendment should only require action upon notification.

To do so, the amendment may state that the interactive computer service shall not be liable for tortious activity of third-party users if the computer service, upon obtaining notification, "acts expeditiously to remove or disable the material."[235] Similar to the DMCA, the amendment should require written notification.[236] Elements of notification should include, in no particular order: (1) identification of the actionable material "reasonably sufficient" to allow the computer service to locate the material;[237] (2) information "reasonably sufficient" to allow the

---

233. *See* 17 U.S.C. § 512(c)(1) (explaining that a service provider escapes liability if it removes or blocks the infringing material upon receipt of actual knowledge or awareness).

234. *See Zeran*, 129 F.3d at 331 ("Another important purpose of § 230 was to encourage service providers to self-regulate the dissemination of offensive material over their services.").

235. *See* 17 U.S.C. § 512(c)(1)(C) (explaining that the service retains liability under the DMCA if "upon notification of claimed infringement . . . , [it] responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity").

236. *See id.* § 512(c)(3)(A) ("To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider . . . .").

237. *See id.* § 512(c)(3)(A)(iii) (listing one element of notification under the DMCA as "identification of the material that is claimed to be infringing . . . and information reasonably sufficient to permit the service provider to locate the material").

computer service to contact the complainant, such as an address, telephone number, or e-mail address;[238] (3) a claim that the listed materials give rise to legal action, such as defamation, invasion of privacy, or a similar civil claim; (4) a statement that the complainant has a good-faith belief that "the use of the material in the manner complained of" gives rise to legal action as described in the claim;[239] and (5) a physical or electronic signature of the complainant.[240]

Because this procedure should provide a simple and efficient means of notification, it may be necessary to create online forms that allow complainants to "check the box" and describe their legal claim. For example, a victim of nonconsensual pornography may not know the various elements of "invasion of privacy," but could check off a list of each of these elements on an online form. Adequate room should be provided for the victim to describe any elements in further detail, or to address a claim not listed in one of the provided forms. To address the possibility of misrepresentation, a clause may be added that imposes liability on any individual who "knowingly materially misrepresents" that material is actionable.[241]

To submit this information, a complainant should be able to turn to the "designated agent" of the computer service.[242] Under the DMCA, computer services must designate an agent to receive incoming notifications of copyright infringement; the DMCA's limitations to liability apply only to services with designated

---

238. *See id.* § 512(c)(3)(A)(iv) (explaining that a complainant must provide "[i]nformation reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted").

239. *See id.* § 512(c)(3)(A)(v) (listing as an element of notification under the DMCA, a "statement that the complaining party has a good-faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law").

240. *See id.* § 512(c)(3)(A)(i) (requiring a "physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed").

241. *See id.* § 512(f) (imposing liability on "any person who knowingly materially misrepresents under this section" that material is infringing or was removed due to mistake or misidentification).

242. *See id.* § 512(c)(2) (requiring that service providers receive notification through "designated agents").

agents.[243] In compliance with the act, the computer services display the contact information for the agent on their website in an accessible location.[244] Similarly, this amendment would require website operators to designate an official agent to receive notifications of civil claims. These agents should be qualified to address the legal claims within the notifications. Because most interactive computer services already have "designated agents" for notification submission, it imposes little hardship to allow submission of additional notifications through those agents or a similar process.

B. Possible Responses to Notification

Upon receipt of notification, a website operator or ISP retains immunity if it follows the procedures set forth in the amendment, but it may lose immunity for failing to promptly address the issue. The legislature may set forth a period of time, such as fifteen days, to allow the service to respond. If a service refuses to respond within the time period and loses its § 230 immunity, the victim may sue the service for the civil claim as though it were the original poster. Though this causes the victim to endure a lengthy and expensive trial, it provides an opportunity for victims to pursue their legal claims against an identifiable defendant who cannot hide behind the shield of § 230 immunity.

Ideally, the ISP or website operator would remove the images within the stated time period, providing the victim with his or her desired relief. To do so, the service must first take reasonable steps to contact the poster and allow that individual to remove the image or gain that individual's permission to remove the image. Understanding the legal consequences of revenge porn postings may incentivize some posters to provide this permission. This allows the interactive computer services to avoid evaluation

---

243. *See id.* ("The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement . . . .").

244. *See id.* (requiring the designated agent's contact information, including name, address, phone number, e-mail address, and other contact information, to be available through the service).

of the legal claim made by the complainant. Avoiding evaluation of the legal claim and providing removal through the poster saves time and may allow removal of more images.

However, attempts to contact the poster may fail due to anonymous postings or the service's inadequate records, or the service may fail to obtain permission for removal. At this point, the service's designated agent would evaluate the legal claim. If the service finds that the claim is colorable, it removes the unlawful material and retains § 230 immunity. However, if the service makes a good-faith determination that the material is not actionable, it must notify the complainant and explain its decision. Unfortunately, some service providers may attempt to abuse this good-faith standard. To protect victims against this particular abuse, the amendment should allow victims to file for injunctive relief at this stage. If a court validates the victim's claim, the victim should be awarded injunctive relief, either in the form of removal or disabling of access to the material; however, the victim would not be able to file a civil suit for damages against the operator.

C. Effectiveness of the Proposed Amendment

This amendment provides a proper remedy for those victims of nonconsensual pornography who cannot find relief under the DMCA or civil and criminal laws that require action against the poster.[245] Though those laws may provide monetary relief or deter future crimes, this amendment provides the remedy that victims actually desire: removal of the harmful images.[246] When the images are removed, they no longer provide access to the victim's social media accounts or home address, and they no longer appear in Google searches or interfere with the victim's employment prospects.[247] This allows the victim to finally move past the harmful online and offline harassment that follows the

245. *See supra* Part III (discussing the limitations of existing legal options).

246. *See supra* note 79 and accompanying text (explaining that victims desire removal more than monetary relief).

247. *See supra* Part II (explaining the economic harms caused by revenge porn).

distribution of these sexually explicit images.[248] Similar to victims pursuing removal of copyrighted images through the DMCA, revenge porn victims may face time-consuming and expensive lawsuits when computer services refuse to act;[249] however, these victims could ultimately find legal recourse in this amendment, either through removal or civil action.

In providing such relief, Congress must address certain constitutional concerns. The DMCA's takedown procedures face few constitutional challenges because copyright infringement finds little protection in the First Amendment;[250] however, takedown procedures within the CDA may attract criticism. Some scholars may argue that speech, especially anonymous speech, on the Internet promotes the dissemination of ideas within a growing public forum.[251] The First Amendment rights of posters, therefore, must be considered when developing responses to nonconsensual pornography. However, in cases of revenge porn and cyber harassment, the rights of the victims must be acknowledged and balanced against the competing First Amendment concerns of posters.[252] When a speaker uses the Internet not for purposes of debate and democratic discourse, or even to spread opinion, but for the purpose of intentionally harassing and harming another individual, courts and the legislature must take notice.[253] Legislatures willingly provide protection for privacy interests in other settings,[254] and Congress

---

248. *See supra* Part II (explaining the harms that stem from the distribution of nonconsensual pornography).

249. *See supra* Part III.A (explaining the limitations of DMCA liability).

250. *See* RODNEY A. SMOLLA, FREE SPEECH IN AN OPEN SOCIETY 144 (1992) (explaining that copyright law requires protection of the copyright interests of the author in order to best protect the free expression of ideas).

251. *See, e.g.*, Richards, *supra* note 229, at 197–99 (explaining courts' protection of anonymous speech on the Internet).

252. *Cf. id.* at 201–04 (noting that courts have created "balancing tests" when a victim of online defamation seeks disclosure of an anonymous poster's identity). These approaches require a balancing of the poster's First Amendment right of anonymous free speech and the prima facie case presented by the victim, as well as the necessity for disclosure. *Id.*

253. *See supra* note 146 and accompanying text (explaining that certain speech is less deserving of First Amendment protection).

254. *See supra* Part III.B (discussing various torts, including misappropriation and invasion of privacy). For example, when criminalizing

must now recognize those interests in the new and unique context of revenge porn and cyber harassment.

Congress should also recognize that this amendment actually furthers its policy goal of protecting speech on the Internet. For example, Congress felt that civil liability would impose such a heavy burden on interactive computer services—who would need to screen millions of posts for tortious activity—that the services might limit the number and type of postings allowed on their sites. This amendment avoids such an "intrusive government regulation of speech" because the ISP or website operator only faces liability after notification. The victim holds an affirmative duty to notify the computer service; therefore, the service will not be forced to regulate millions of user accounts to track down tortious activity, nor will it be forced to limit speech on its site.

In *Zeran*, the Fourth Circuit expressed concern with liability upon notification.[255] The court noted, "If computer service providers were subject to [liability upon notification], they would face potential liability each time they receive notice of a potentially defamatory statement . . . ."[256] The court continued to explain that this causes a "careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information."[257] This proposed amendment addresses these concerns in a variety of ways. First, the service may avoid an evaluation of the legal claim by contacting the poster and receiving permission to remove the material. If this proves ineffective, the service must address the legal claim, but it does so through its designated agent. The amendment provides a reasonable period of time (to

---

voyeurism, New Jersey noted that "people have a right to control the observation of their most intimate behavior under circumstances where a reasonable person would not expect to be observed." S. Comm. State., S.B. 2366, 210th Leg., at 1 (N.J. 2013).

255. *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997) (explaining the problems of imposing liability upon notification, or "distributor liability").

256. *Id.*

257. *Id.*

be determined by the legislature) to allow for evaluation of the claim and response by the service. While services face "potential liability each time they receive notice," they are faced with a variety of options to address these notifications and respond to the complainant without losing their § 230 immunity.

Furthermore, this amendment encourages interactive computer services to take action against unlawful activity, which supports Congress's primary goal of "targeting indecency on the Internet and encouraging ISPs to block and filter objectionable material."[258] Current interpretations of § 230 immunity provide no such incentive for self-regulation.[259] Rather, ISPs and website operators receive immunity regardless of whether they act upon notification and may simply ignore victims' pleas to remove actionable material.[260] This allows tortious and harmful material to thrive on these sites. This amendment would require ISPs and website operators to act upon notification, and the threat of civil liability would encourage the computer services to thoughtfully consider the notification and remove the objectionable materials.[261]

VI. Conclusion

The Seventh Circuit once asked, "Why should a law designed to eliminate ISPs' liability to the creators of offensive material end up defeating claims by the victims of tortious criminal conduct?"[262] Though the court ultimately followed the traditional

258. *See* Duran, *supra* note 169, at 125 (explaining that the CDA "has worked against [Congress's] primary goal of targeting indecency on the Internet and encouraging ISPs to block and filter objectionable materials").

259. *See, e.g.*, *id.* (providing examples of courts' refusal to impose liability on computer services even after the service fails to act after receiving notification of harmful material). For example, in *Doe v. GTE Corp.*, ISP personnel may have been aware of obscene images of college athletes recorded by a hidden camera, but the lawsuit was dismissed. Doe v. GTE Corp. 347 F.3d 655, 662 (7th Cir. 2003).

260. *See, e.g.*, *Zeran*, 129 F.3d at 333 (finding for defendant computer service despite its failure to act upon notification of harmful material).

261. *See* Duran, *supra* note 169, at 124 ("The threat of lawsuits would force an ISP to at least review complaints and respond to problems.").

262. *Doe*, 347 F.3d at 660.

broad interpretation of § 230 and granted immunity to the defendant ISP in that case,[263] it raised an important point: when interactive computer services like websites and ISPs retain civil immunity despite knowledge of unlawful conduct by third-party posters, they allow harmful activities to flourish on the Internet.[264] This includes the distribution of nonconsensual pornography, but also extends to cyberbullying, cyber harassment, and cyber stalking as well.[265] These activities continue without much regulation by website operators or ISPs, and victims find that their relief is barred by the broad interpretations of § 230 immunity as well as by inadequate and inefficient relief in other areas of law. This immunity leads to an endless cycle of unfettered tortious activity on the web.

While some states seek criminal prosecution of posters to combat nonconsensual pornography, an amendment to § 230 requiring action upon notification provides a more comprehensive and effective remedy. Such an amendment not only provides victims with the removal they seek, but it also incentivizes regulation of tortious material, rather than supporting a completely hands-off approach. This halts the cycle of online tortious activity that affects the lives of so many and begins instead a process of healing for victims of online abuse.

---

263. *See id.* at 662 (affirming the lower court's dismissal of the case in favor of the defendant computer service).

264. *See* Citron, *supra* note 62, at 119 ("[B]road immunity for operators of abusive websites eliminates incentives for better behavior by those in the best position to minimize harm." (citation omitted)).

265. *See id.* at 68–84 (describing various incidents of online harassment and abuse).