Protecting Does and Outing Mobsters: Recalibrating Anonymity Standards in Revenge Porn Proceedings

ELIZABETH BROWN*

INTRODUCTION

Nonconsensual porn, popularly known as revenge porn[1], is becoming an epidemic without an effective and coherent legal remedy. As its name suggests, it is the posting or distribution of sexually explicit images without the consent of the person purportedly represented in those images, sometimes by anonymous sources. In recent years, both the incidence of its distribution and the severity of its consequences have risen dramatically. A recent study suggests that one in eight social media users has been a victim of nonconsensual porn, and that women are 1.7 times more likely to be targeted than men.[2] According to a 2016 report, one in twenty-five U.S. residents have either been victims of nonconsensual porn or have been threatened with posting sensitive images without their consent.[3] That number rises to one in eight for women between the ages of 15 and 29.[4] Nonconsensual porn victims may suffer a wide range of harms, including professional, reputational and economic harms that are often impossible to remedy in full because the offensive images can never be permanently erased. In November 2017, New York City passed a new nonconsensual porn law.[5] In doing so, it joined a national trend of new regulations concerning nonconsensual porn.[6] This increase reflects a growing concern about nonconsensual porn but these new laws do not go far enough in providing an effective recourse for its victims.

---

* Assistant Professor, Department of Law, Taxation and Financial Planning, Bentley University.

1. Professors Clare McGlynn and Erika Rackley advocate for replacing the term "revenge porn" with the term "image-based sexual abuse." *See* CLARE MCGLYNN & ERIKA RACKLEY, SUBMISSION ON THE ABUSIVE BEHAVIOUR AND SEXUAL HARM (SCOTLAND) BILL 2015, (ABSH 3) § 3 (Nov. 2015) http://www.parliament.scot/parliamentarybusiness/CurrentCommittees/93304.aspx; Clare McGlynn & Erika Rackley, *Not Porn, but Abuse: Let's Call it Image-Based Sexual Abuse*, EVERYDAY VICTIM BLAMING (Mar. 9, 2016), http://everydayvictimblaming.com/media-complaints/not-revenge-porn-but-abuse-lets-call-it-image-based-sexual-abuse-by-%e2%80%8fmcglynnclare-erikarackley/.

2. *Nonconsensual Porn: A Common Offense*, CYBER CIVIL RIGHTS INITIATIVE (June 12, 2017),https://www.cybercivilrights.org/2017-natl-ncp-research-results/. Because women are significantly more likely to be victims of NCP, I use the feminine pronoun when referring to NCP victims in this article even though both men and women may be targets.

3. AMANDA LENHART ET AL., DATA & SOC'Y RESEARCH INST., NONCONSENSUAL IMAGE SHARING: ONE IN 25 AMERICANS HAS BEEN A VICTIM OF REVENGE PORN 3 (2016).

4. *Id.* at 5.

5. Sara Ashley O'Brien, *Revenge Porn Will Soon Be a Crime in New York City*, CNN MONEY: TECH (Nov. 16, 2017), http://money.cnn.com/2017/11/16/technology/nyc-revenge-porn-bill/index.html.

6. *See infra* notes 116–122 and accompanying text.

While new laws are being enacted with greater urgency at the state and local levels, these new laws are lacking in two specific and critical ways. First, they do too little to shield victims from the retaliation and reprisals that often accompany nonconsensual porn claims. Victims may be unwilling to take advantage of their new legal recourses because they may reasonably fear the additional harassment that may result from exposing their identity and personal information. At the same time, victims may be unwilling or unable to meet the higher burden involved in suing anonymously, since current procedural standards for suing pseudonymously generally require a would-be "Plaintiff Doe" to meet a higher evidentiary standard than she would if she used her real name.

The second challenge is that many putative nonconsensual porn defendants are anonymous, and it is more difficult and more expensive to sue defendants whose real identity is unknown. This is partly because the procedural standards for unmasking anonymous defendants are unreasonably cumbersome, and partly because internet content providers (ICPs), including social media companies like Facebook, Google, and Twitter, have little incentive to disclose users' real identities voluntarily. The Communications Decency Act (CDA) provides a safe harbor for them that works against the interests of victims and law enforcement, and should be reevaluated.

Both the challenge of hesitant plaintiffs/complainants and the challenge of identifying anonymous defendants can be resolved by recalibrating the extent to which anonymity is tolerated in nonconsensual porn cases. This article argues that traditional preferences for anonymity should be reexamined in light of the pervasive and permanent damages nonconsensual porn causes and the difficulty of framing these damages in the strictly economic terms most familiar to courts. Anonymity is considered a right on social media, but a privilege in the justice system. In the context of revenge porn, it may be time to flip those standards.

This article joins a growing discussion of the wisdom of current standards for pseudonymous plaintiffs and augments it by focusing on the unique circumstances of revenge porn victims. It comparatively evaluates public and private remedies in order to develop recommendations for more effective and protective remedies for victims of nonconsensual porn, and makes three specific recommendations. The first is to revise and standardize the conditions under which a victim may shield her identity and personal information when alleging nonconsensual porn, either as a plaintiff in a civil case or in a criminal prosecution on her behalf. The second is to refine, and in some cases relax, the current standards for compelling ICPs to disclose the names of anonymous alleged nonconsensual porn perpetrators. The third is to expand potential liability for ICPs when they fail to respond reasonably once they are put on notice that they may be facilitating nonconsensual porn.

The changing nature of hiring practices and practical permanence of social media personae should inform judicial decisions about balancing the interests of the plaintiff, the defendant, the public, and the ICPs facilitating this harm. In light of the weak protections current public laws and private policies offer victims of nonconsensual porn, other options should be considered. As one scholar wrote in another context, "[t]o preserve constitutional rights and access to justice, legal systems must provide well-functioning mechanisms to check against

intimidation—especially when fear generated by past reprisals may be keeping people out of court."[7] In the context of nonconsensual porn, victims require more anonymity and accused perpetrators require less. As for social media companies, it is a relatively small but important step to require them by law to engage in the kind of curbing efforts they have begun to take on voluntarily.

I. THE UNIQUE PROLIFERATION AND CONSEQUENCES OF NONCONSENSUAL PORN MANDATE RECONSIDERING PRIVACY FOR PLAINTIFFS AND DEFENDANTS

Nonconsensual porn is an often permanently damaging form of privacy invasion that affects a growing number of internet users, more often women than men. Under the name "revenge porn," it has grabbed headlines in recent years. In early 2017, the nonconsensual posting of sexually explicit photos of female Marines without their consent on the Marines United Facebook page created a scandal and prompted an investigation by the Pentagon.[8] Later in 2017, Rob Kardashian posted sexually explicit photographs of his ex-girlfriend, Blac Chyna, on Instagram, apparently in anger over her affair with another man.[9] When Instagram took them down, Kardashian posted other nonconsensual porn images of Chyna on Twitter.[10] Another minor celebrity, Mischa Barton, sued two men in 2017 in an effort to block their unauthorized distribution of nude photos and videos of her.[11]

Most victims of nonconsensual porn, of course, are not nearly as famous and would prefer to keep it that way. In fact, a critical harm of nonconsensual porn is the unwanted exposure of a victim's identity and personal details, along with her name, promulgated to the public at large, sent specifically to her friends, family, and/or co-workers.[12]

While headline stories involving celebrities like Kardashian and Barton involved in nonconsensual porn litigation have brought a certain amount of attention to the issue, legal solutions are lagging behind. The unique nature of nonconsensual porn compared with other torts makes it necessary to reconsider the unreasonably high burden courts have placed both on plaintiffs who want to sue pseudonymously and plaintiffs who try to unmask anonymous defendants in the context of nonconsensual porn claims.

---

7. Benjamin P. Edwards, *When Fear Rules in Law's Place: Pseudonymous Litigation as a Response to Systematic Intimidation*, 20 VA. J. SOC. POL'Y & L. 437, 440 (2013).

8. Bill Chappell, *Sharing of Nude Photos of Female Marines Online Prompts Pentagon Investigation*, NPR: THE TWO-WAY (Mar. 6, 2017, 8:10 AM), http://www.npr.org/sections/thetwoway/2017/03/06/518767235/sharing-of-nude-photos-of-female-marines-prompts-pentagon-investigation.

9. Edgar Alvarez, *Rob Kardashian's Revenge Porn is Social Media's Latest Headache*, ENGADGET (July 11, 2017), https://www.engadget.com/2017/07/11/rob-kardashian-blac-chyna-revenge-porn/.

10. *Id.*

11. *Mischa Barton Reaches Settlement in Revenge-Porn Case*, CBS LOS ANGELES (June 5, 2017, 4:19 PM), http://losangeles.cbslocal.com/2017/06/05/mischa-barton-revenge-porn/.

12. *See infra* notes 17–26 and accompanying text.

A. Nonconsensual Pornography Is Increasingly Pervasive

Nonconsensual porn is a form of digital sexual harassment and a turbocharged invasion of physical and sexual privacy.[13] It is sometimes defined as a sex crime and sometimes as a basis for civil liability.[14] Nonconsensual porn is generally defined as the distribution of images of a fully or partially naked person, purporting to be of the victim without the victim's consent, without necessarily having a specific motivation to harm.[15] Revenge porn differs from nonconsensual porn, in that it assumes a motive to harass, disturb, or otherwise intentionally harm the victim.[16]

In one manifestation of nonconsensual porn, sexually explicit photos of a victim are distributed without the victim's consent, sometimes to the victim's friends, family, and co-workers.[17] In some cases, the photos were taken privately, or were derived from webcams switched on without the subject's knowledge.[18] In other cases, the images are created by photoshopping a victim's head onto someone else's nude body, and the photo purports to be a naked image of the victim.[19] One of the most damaging aspects of nonconsensual porn cases is the frequency with which personal information such as home and email addresses are posted alongside the nude images. This practice, called doxing or doxxing, is a common feature in nonconsensual porn. According to one source, personal identifying information is posted with nonconsensual porn images nearly sixty percent of the time.[20] The nonconsensual porn images pop up in internet searches of the victim's name, sometimes causing victims to lose their jobs or to have difficulty applying for jobs because of the results that come up when employers or potential employers search for their names online.[21]

Nonconsensual porn images can spread across the internet easily. A poster can disseminate an image instantaneously, and that image may dominate search engine results for the victim within days.[22] This is exacerbated by thousands of

13. *See* Adrienne N. Kitchen, Note, *The Need to Criminalize Revenge Porn: How a Law Protecting Victims Can Avoid Running Afoul of the First Amendment*, 90 CHI.-KENT L. REV. 247, 292 (2015).

14. *See* Charlotte Alter, *'It's Like Having an Incurable Disease': Inside the Fight Against Revenge Porn*, TIME: SOCIETY (June 13, 2017), http://time.com/4811561/revenge-porn/.

15. *See Nonconsensual Porn: A Common Offense supra* note 2.

16. Alter, *supra* note 14.

17. *Id.*

18. *Id.*

19. There is, effectively, a minor industry in photoshopping one person's head onto another person's naked body, including for the purposes of revenge porn. *See* Kashmira Gander, *The People Who Photoshop Friends and Family Onto Porn*, INDEPENDENT: INDY/LOVE (Oct. 13, 2016, 9:30 AM) http://www.independent.co.uk/life-style/love-sex/porn-photoshopping-4chan-family-friends-superimposed-into-sex-scenes-world-a7358706.html.

20. *What Makes an Effective Revenge Porn Law?*, C.A.GOLDBERG, http://www.cagoldberglaw.com /what-makes-an-effective-revenge-porn-law/ (last visited Jan. 16, 2018).

21. Lorelei Laird, *Victims Are Taking on 'Revenge Porn' Websites For Posting Photos They Didn't Consent To*, ABA JOURNAL (Nov. 2013), http://www.abajournal.com/magazine/article/victims_are_taking_on_revenge_porn_websites_for_posting_photos_they_didnt_c.

22. MARY ANNE FRANKS, CYBER CIVIL RIGHTS INITIATIVE, DRAFTING AN EFFECTIVE "REVENGE PORN" LAW: A GUIDE FOR LEGISLATORS2 (Aug. 2015) https://www.cybercivilrights.org/wp-content/uploads/2016/09/Guide-for-Legislators-9.16.pdf.

websites which are dedicated to revenge porn.[23] The images are further spread by what some scholars have called an "amplification effect," in which mobs of people compete with each other to see who can create the most damaging images or other harassment of the victim.[24] The "amplification effect" refers to the subsequent reposting and sharing of the initial post, which is often done by groups competing "to outdo each other" and "be the most offensive, the most abusive."[25] As a result of this competition, the initial post quickly spreads in reach and grows in offensive content, with subsequent posters adding sexual slurs and personal information about the victim. The number of viewers increases exponentially as it spreads. The victim typically only has a legal remedy against the initial poster, and not against the legion of re-posters.[26] Internet archiving makes this worse, in that the harmful images and comments can stay online, and come up in searches, indefinitely. Victims of nonconsensual porn often have no definitive measure of how widely their private images have spread.

Internet content providers, including social media sites such as Facebook, are struggling to deal with the viral spread of revenge porn. Documents leaked to the media suggested that Facebook had to assess almost 54,000 cases of reported revenge porn in a single month.[27] Because Facebook relies on user reports to flag instances of revenge porn, the number of potential revenge porn postings could be higher.[28] Facebook is trying to prevent users from posting some explicit content by using "image-matching" software, but claims to have trouble distinguishing between acceptable and unacceptable material.[29] Facebook is also adapting new and somewhat controversial technologies for flagging and removing nonconsensual porn.[30]

The private nature, irreversible harms and online amplification of nonconsensual porn make it unlike other crimes. Kara Jefts, an academic and art historian at a Chicago university, became a victim of nonconsensual porn when she ended a long-term relationship with a boyfriend.[31] Soon after the split, he posted sexually explicit images taken from their Skype conversations online to Facebook, together with violent threats against Jefts.[32] These images were emailed to Jefts' friends and family and uploaded to websites aimed at exposing the sexually transmitted diseases of individuals, with misinformation about Jefts'

---

23. *Id.*(noting that as many as 3,000 websites feature revenge porn); Dylan Love, *It Will Be Hard to Stop the Rise of Revenge Porn*, BUSINESS INSIDER AUSTRALIA: TECH INSIDER (Feb. 8, 2013, 11:00 am) https://www.businessinsider.com.au/revenge-porn-2013-2.

24. Apeksha Vora, Note, *Into the Shadows: Examining Judicial Language in Revenge Porn Cases*, 18 GEO. J. GENDER & L. 229, 230 (2017).

25. *Id.*

26. *Id.*at 231.

27. Nick Hopkins & Olivia Solon, *Facebook Flooded With 'Sextortion' and 'Revenge Porn', Files Reveal*, THE GUARDIAN (May 22, 2017, 9:52 AM), https://www.theguardian.com/news/2017/may/22/facebook-flooded-with-sextortion-and-revenge-porn-files-reveal.

28. *Id.*

29. *Id.*

30. *See* discussion *infra* Section IV(B).

31. Alter, *supra* note 14.

32. *Id.*

sexual past.[33] Internet searches of Jefts' name were subsequently dominated by information about Jefts' status as a victim, causing irreversible damage to her personal and professional reputation.[34] "I have to accept at this point that it's going to continue to follow me," she told Time magazine.[35] "It's kind of like having an incurable disease."[36]

Nonconsensual porn is one of many harms perpetuated in part by the online environment. More than ninety percent of internet users agree that there is something about the online environment that allows people to be more critical of each other,[37] often in dangerous ways. According to a study by the Pew Research Center, a full seventy-three percent of adults have seen someone else be harassed online and forty percent have experienced harassment online themselves.[38] Of course, not all harassment is equally severe. The study differentiated between less severe harassment, which includes name-calling and more common annoying behaviors, and more severe harassment, which includes physical threats, sustained harassment over time, and sexual harassment.[39] Of those who had been harassed online, the survey found that forty-five percent of them, or eighteen percent of all internet users, experienced the more severe form of harassment.[40]

Young women between the ages of 18 and 24 experience stalking and online sexual harassment at "disproportionately high levels," according to the study.[41] Of these women, twenty-six percent report having been stalked, twenty-five percent report having been sexually harassed, and twenty-three percent of them reported having been physically threatened.[42] Social media is a particularly risky environment in this context. Two-thirds of internet users surveyed said that their most recent incidence of harassment occurred on a social networking website or app.[43]

Similarly, women are more vulnerable to the use of nonconsensual porn than men. Estimates of the percentage of revenge porn victims who are female range from sixty to seventy percent, on the low end, to more than ninety percent.[44] In the first nationwide study of nonconsensual porn, women were "significantly more likely" (about 1.7 times as likely) to have been subject to nonconsensual

---

33. *Id.*

34. *Id.* An internet search of "Kara Jefts" conducted on November 16, 2017 returned information about Ms. Jefts' experience as a victim of revenge porn as well as professional information about her.

35. *Id.*

36. *Id.*

37. PEW RESEARCH CENTER: INTERNET & TECH REPORT, ONLINE HARASSMENT 8 (Oct. 22, 2014), http://assets.pewresearch.org/wp-content/uploads/sites/14/2014/10/PI_OnlineHarassment_72815.pdf.

38. *Id.* at 2.

39. *Id.*

40. *Id.*

41. *Id.* at 3.

42. *Id.*at 3–4.

43. PEW RESEARCH CENTER, *supra* note 37, at 5–6. The survey distinguished social media websites and apps from dating websites and apps.

44. *See, e.g.*, Eaton, *infra* note 45, at 13 (noting that women are 1.5 times more likely to report being victims than men), Citron, *infra* note 55, at 17 (noting a study finding that ninety percent of victims were women).

distribution of their naked images or threatened with such distribution than men.[45] Nearly sixteen percent of all women participating in the study reported having been victimized or threatened, compared with just over nine percent of men.[46] Women were even more likely than men to experience threats of nonconsensual porn distribution than men, with 6.6% of women reporting threats compared with only 2.6% of men.[47]

While attracting scholarly attention, nonconsensual porn is also subject to the subtle marginalization of crimes with predominantly female victims. "The trivialization of women's harms is not new," writes Apeksha Vora in an article examining what she describes as the trivializing languages judges use to describe the harm in revenge porn opinions.[48] "[S]ociety often discounts harms that disproportionately affect women, as is seen most clearly in the historical treatment of rape, domestic violence, and sexual harassment in the workplace."[49] Given the popular misconception that there is a right to be anonymous on the internet, the concerns of nonconsensual porn victims may suffer even more in comparison.

In addition to the psychological, economic, and professional damages individual victims suffer, nonconsensual porn also hurts society. When the victims are people who already feel marginalized by social discourse, being harassed online makes them even less likely to participate in online dialogues. At least one study suggests that women, people of color, lesbians, gays and bisexuals already are more likely to censor themselves online than heterosexual white men because they have a greater fear of consequent online harassment.[50] As a result, social discourse overall becomes less diverse and skews in favor of those who feel more powerful and privileged. This is a serious loss, although the impact is difficult to quantify. Limiting the scope of people who feel able to participate fully in social discourse risks creating a segment of the population that is "chronically dogged by a spoiled social identity, and a much larger class of people who know that they could be subjected to such treatment without hope of redress."[51] This outcome would run "directly afoul of the ideal of a regime that allows for confidence, empowerment, and agency in the forum of public debate."[52] The consequences of nonconsensual porn, therefore, are dangerous for a free and open society as a whole.

---

45. ASIA A. EATON ET AL., CYBER CIVIL RIGHTS INITIATIVE, 2017 NATIONWIDE ONLINE STUDY OF NONCONSENSUAL PORN VICTIMIZATION AND PERPETRATION 12 (2017), https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf.

46. *Id.*

47. *Id.* at 14.

48. Vora, *supra* note 24, at 248.

49. *Id.*

50. AMANDA LENHART ET AL., DATA & SOC'Y RESEARCH INST.ONLINE HARASSMENT, DIGITAL ABUSE AND CYBERSTALKING IN AMERICA 53 (Nov. 21, 2016).

51. Andrew Koppelman, *Revenge Pornography and First Amendment Exceptions*, 65 EMORY L.J. 661, 663 (2016).

52. Ashton Cooke, Note, *The Right to Post: How North Carolina's Revenge Porn Statute Can Escape Running Afoul of the First Amendment Post-*Bishop, 15 FIRST AMEND. L. REV. 472, 484 (2017).

B. Revenge Porn Causes Extensive and Often Irremediable Damages

The harm inflicted by the viral spread of nonconsensual porn may include psychological, economic and reputational damages that are qualitatively different from traditional tort damages, particularly in their permanence. These damages may surprise legal scholars unfamiliar with the unique dynamics of nonconsensual porn. In fact, the intractability of harm caused by nonconsensual porn would be all but unrecognizable to tort law commentators in the mid-twentieth century. Now, approximately seventy-five percent of all Americans use the internet.[53] As more social and economic aspects of our lives move online, the potential damage caused by these kinds of online comments and postings becomes more extreme and inescapable.

Nonconsensual porn in particular can cause damage that is severe, pervasive, and often nearly impossible to remedy completely. Victims are "frequently threatened with sexual assault, stalked, harassed, fired from jobs, and forced to change schools."[54] False comments, doctored images, and images distributed without consent can make victims feel powerless and depressed. Some receive death threats. Others are forced to relocate.[55]

In one example, a victim who wanted to remain anonymous reported that she began to suffer the effects of nonconsensual porn posted by her ex-husband, whom she divorced in 2009.[56] Three years later, she was working for a Fortune 500 company when she started receiving hundreds of text messages and friend requests from people she did not know.[57] She alleges that her ex-husband posted an intimate photo he took of her on their wedding night on a public forum together with pictures of her daughter, her workplace, and her email address.[58] Men began to call her on her company's customer service line, trying to extort money and threatening her family.[59] She spent $7,500 in an effort to remove the pictures, but they were continually reposted on different websites.[60] The FBI were unable to help her effectively until her state passed a nonconsensual porn law in 2015, under which her ex-husband was arrested, pleaded guilty, and was sentenced to prison time.[61] Despite his conviction, she still received harassing messages from strangers on Facebook.[62]

Negative online comments and images can have devastating professional consequences. This is increasingly so, given that employers regularly conduct

---

53. *Internet Users (per 100 People)*, UNDATA, http://data.un.org/Data.aspx?d=WDI&f=Indicator_Code%3aIT.NET.USER.P2%3bCountry_Code%3aUSA&c=2,4,5&s=Country_Name:asc,Year:desc&v=1 (last visited Feb. 10, 2018).

54. Franks, *supra* note 22, at 2.

55. DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 6-7 (2014) [hereinafter CITRON, HATE].

56. Kaitlin Rust, *"Revenge Porn" Victim Speaks Out After Ex-husband Is Convicted*, KPLC (Dec. 11, 2017), http://www.kplctv.com/story/37042582/revenge-porn-victim-speaks-out-after-ex-husband-is-convicted.

57. *Id.*

58. *Id.*

59. *Id.*

60. Rust, *supra* note 56.

61. *Id.*

62. *Id.*

online searches and social media audits before extending interview and job offers.[63] Revenge porn victims report losing their jobs when their employers see the images posted and losing job opportunities when potential employers see these images. In complaints to the FTC, victims alleged that their employers received phone calls alerting them to where the victims' photographs were posted online.[64] Other victims despaired that the nonconsensual porn images were the first results that came up in Google searches of their names.[65]

The reputational damage caused by online speech can have serious consequences beyond the professional realm. According to a 2014 study, one-third of victims of the more severe forms of online harassment believe that their reputation has been damaged as a result of that harassment.[66]

C. Victims Cannot Fix, Forget or Fight Online Harassment

Nonconsensual porn victims have limited resources outside of the legal system. In the United States, there is no statutory "right to forget" as there is in many European countries.[67] Some victims seek help from advocacy organizations such as the Cyber Civil Rights Initiative, which receives between twenty and thirty such requests every month.[68] In general, victims have three options: fix it, forget it, or fight it. As described below, none of these is truly satisfactory, but there are ways to make at least one of them more effective.

A nonconsensual porn victim's first option is to try to fix the problem, primarily by removing the offending images and information from the internet. Reputation management companies offer to help, for a fee, by using search engine optimization that pushes positive content about a person to the top of a search result and therefore makes it less likely that negative results will come up quickly. One such company, Reputation Defender, offers packages that range in price between $3,000 and $25,000 for the basic service level.[69]

Reputation management companies have reputation problems of their own, however. Some victims of nonconsensual porn will hesitate to use them in light of a widely publicized scheme involving a firm called Change My Reputation.[70] This firm was run by Kevin Bollaert, who simultaneously operated a revenge porn site called UGotPosted.com.[71] When victims complained about their images on

63. CITRON, HATE, supra note 5, at 7-9.

64. Complaint for Permanent Injunction and Other Equitable Relief at 15, Fed. Trade Comm'n v. EMP Media, Inc., No. 2:18-cv-00035 (D. Nev. Jan. 9, 2018) https://www.ftc.gov/system/files/documents/cases/1623052_myex_complaint_1-9-18.pdf.

65. *Id*.

66. PEW RESEARCH CENTER, *supra* note 7, at 7.

67. Jeff John Roberts, *The Right To Be Forgotten From Google? Forget It, Says U.S. Crowd*, FORTUNE: TECH (Mar. 12, 2015), http://fortune.com/2015/03/12/the-right-to-be-forgotten-from-google-forget-it-says-u-s-crowd/.

68. Franks, *supra* note 22, at 2.

69. *Personal Online Reputation Management*, REPUTATION DEFENDER, https://www.reputationdefender.com/reputation (last visited Feb. 10, 2018).

70. Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 368–69 (2014).

71. *Id*. at 368.

UGotPosted, Bollaert directed them to Change My Reputation, which then charged the victims between $250 and $350 to remove their images.[72] Bollaert and his colleague were later ordered to pay one victim $385,000 in compensatory and punitive damages.[73] In another more recent example, the FTC investigated a website called MyEx.com, which solicited pictures, videos and personal information of victims and urged visitors to "Submit Pics and Stories of Your Ex."[74] The site then allegedly charged several victims between $500 and $2,800 to remove their images and information.[75]

A second option is for nonconsensual porn victims to try to forget what has been done to them and avoid the images altogether. Revenge porn, however, is usually inescapable. It is not practical for a victim to simply stay off social media because of its ubiquity in modern life. The mob mentality of nonconsensual porn promoters makes it likely that offending images will spread rather than evaporating. The popularity of websites dedicated to revenge porn, such as UGotPosted and MyEx, contributes to this phenomenon. Even if it were feasible for victims to stay offline, the larger consequence may be the departure of primarily young females and other members of marginalized groups from the realm of online discussions, an outcome which is neither socially desirable nor particularly just.[76]

A third option is for victims to fight back. Given our legal system's preference for open fora, one traditional response to the notion that hate speech can cause harm has been to observe that more speech can counter it.[77] As Justice Louis Brandeis wrote in a 1927 case concerning the extent to which certain speech posed a threat to society, "the remedy to be applied is more speech, not enforced silence."[78] But this is not feasible in the context of revenge porn. Revenge porn victims cannot meet their harassers with equal and opposite force. A woman whose naked image has been disseminated across the internet faces social, economic, and professional repercussions that may last for years. A girl who faces online harassment usually cannot fight back with equal and opposing harassment, even if we would want her to as a matter of social policy, especially if she has no idea who harassed her in the first place. More speech does not help a woman whose home address has been disclosed, or one whose children's names and schools have been broadcast alongside private images of her. The victims' inability to counter their harassment with more speech is especially great when their harassers' identity is unknown.

---

72. *'Revenge Porn' Site Ordered to Pay Ohio Woman $385,000*, NBC NEWS (Mar. 19, 2014 9:42 PM), http://www.nbcnews.com/news/us-news/revenge-porn-site-ordered-pay-ohio-woman-385-000-n57276.

73. *Id*.

74. *FTC and Nevada Seek to Halt Revenge Porn Site*, FED. TRADE COMM'N (Jan. 9, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/ftc-nevada-seek-halt-revenge-porn-site.

75. *Id.*

76. Alice Marwick, *A New Study Suggests Online Harassment is Pressuring Women and Minorities to Self-Censor*, QUARTZ (Nov. 24, 2016), https://qz.com/844319/a-new-study-suggests-online-harassment-is-pressuring-women-and-minorities-to-self-censor/.

77. *See, e.g.,* Franklyn Haiman, *The Remedy Is More Speech*, AMERICAN PROSPECT (Summer 1991), http://prospect.org/article/remedy-more-speech.

78. Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

The unique nature of nonconsensual porn's viral spread, permanence, and harm requires a unique legislative and procedural approach. At a minimum, it is necessary for scholars and legislators to reconsider whether our traditional assumptions about anonymity should be challenged in this context. Civil plaintiffs and criminal complainants are required or strongly encouraged to disclose their identities, while people accused of civil violations or criminal acts enjoy more anonymity and protection from unmasking. It may be sensible to moderate both of those presumptions in the context of nonconsensual porn.

II. NONCONSENSUAL PORN VICTIMS NEED GREATER PRIVACY FOR FULL ACCESS TO JUSTICE

Anonymity affects nonconsensual porn victims and perpetrators in opposite ways. Anonymity is, to some extent, a right protected by the First Amendment. The Supreme Court has recognized the right to speak anonymously as part of the right of free speech.[79] Anonymity in judicial proceedings, however, is subject to a complex and variable set of rules, as described below. In the context of remedying nonconsensual porn harms, this article is primarily concerned with two kinds of anonymity issues: suing pseudonymously, also known as suing as "Plaintiff Doe," and uncovering the identity of an anonymous defendant. There is no uniform federal standard for suing under a pseudonym, nor is there a uniform federal standard for unmasking an anonymous source of alleged nonconsensual porn. The complexity of rules surrounding each aspect of nonconsensual porn litigation exacerbates the difficulty of bringing alleged nonconsensual porn tortfeasors and criminals to justice.

Effectively limiting nonconsensual porn requires consideration of two changes. The first is to make it safer for victims who fear retaliation to use both the civil and criminal channels of the legal system by allowing them to proceed without disclosing their true identity. The second is to make it easier to identify anonymous perpetrators of nonconsensual porn, a remedy that may require the participation of ICPs. The first of these suggestions is explored here in Section II, and the second follows in Section III.

A. Nonconsensual Porn Victims Face Significant Difficulties in Securing Legal Rights

In the context of nonconsensual porn, anonymity works for the accused and against the accuser. Current standards make it all but impossible for a victim of anonymous online harassment to take a legal stand against harassers that she cannot identify. Anonymity online offers a cloak of protection for nonconsensual porn perpetrators because there is relatively little risk that their identity will be disclosed and that they will therefore be subject to criminal or civil liability.

79. *See, e.g.*, Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. Of Stratton, 536 U.S. 150, 166–67 (2002) (finding that a law requiring a permit to distribute pamphlets door-to-door was unconstitutional because it infringed on the speaker's First Amendment rights); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341–42 (1995) ("[T]he anonymity of an author is not ordinarily a sufficient reason to exclude her work product from the protections of the First Amendment.").

No such protection is available to victims of nonconsensual porn in most cases. A limiting factor in curbing nonconsensual porn is the reluctance of victims to come forward, often because they fear further retaliation. This fear is reasonable, given the mob mentality encouraged by many of the websites dedicated to revenge porn, and the increasingly common practice of competing to see who can hound victims most effectively.[80]

One measure that might pave the way for more legal challenges to online harassment would be to relax the requirements for filing a lawsuit pseudonymously. Being able to remain anonymous might make it easier for victims of severe online harassment to sue their attackers. Online harassment victims may hesitate to sue their attackers in part because they do not want to suffer from the increased attention, and potentially increased harassment, that comes with filing a lawsuit. Many victims of nonconsensual porn are too ashamed to come forward, or reluctant to admit that sexually explicit photos were taken of them under any circumstances, even though the practice of sending nude pictures is increasingly common, especially among young women.[81] According to one survey, thirty-seven percent of teenage girls say that they have sent nude or semi-nude photos by text, email or IM, while fifty-six percent of women age 20-26 say that they have done so.[82]

A key limitation of these theories is the understandable hesitation of nonconsensual porn victims to expose themselves to the mob exacerbation and doxxing that usually accompany publicized examples of nonconsensual porn. As discussed below, the standards for pleading under a pseudonym in civil cases vary widely and often impose dauntingly high burdens of proof for the applicant in comparison with named plaintiffs. Although most states have enacted nonconsensual porn-specific laws within the last several years, few of them provide the kinds of anonymous pleading provisions that would make it easier for nonconsensual porn victims either to file civil lawsuits on their own or to become victim-witnesses in criminal prosecutions under those laws.

B. Putative Doe Plaintiffs Face Variable Pleading Standards

Nonconsensual porn victims have been able to use various traditional legal claims to address this nontraditional harm, at least in theory. Scholars have suggested the expanded use of largely tort-based remedies, including claims for invasion of privacy, as well as copyright infringement.[83] While the First Amendment protects against government regulation of some speech, not all speech is protected to the same extent. Unlawful surveillance, cyber-stalking, child pornography (if the subject is under 18) and hacking (if the images were taken using the subject's phone or computer without consent) all may be potential bases of liability in cases like these.[84] The definitions of cyber-harassment and

80. Vora, *supra* note 24, at 230–31.

81. *Sexting Statistics*, STATISTIC BRAIN, http://www.statisticbrain.com/sexting-statistics/ (last visited Jan. 16, 2018).

82. *Id.*

83. *See* Scott D. Camassar, *Cyberbullying and the Law: An Overview of Civil Remedies*, 22 ALB. L.J. SCI. & TECH. 567 (2012).

84. *Related Laws*, CYBER CIVIL RIGHTS INITIATIVE, https://www.cybercivilrights.org/related-laws/

cyber-stalking vary from state to state, however, as do the accompanying standards for determining the accused's intent.[85]

Another legal basis for combating nonconsensual porn may be an increase in the penalties associated with civil rights violations or hate speech in certain cases. These enhanced penalties could attach to speech that (1) causes or is likely to cause certain kinds of harm, or (2) targets religious and/or sexual identity. In a 2014 book, Danielle Citron argued that because online harassment targets women and minorities disproportionately and limits their freedom of self-expression, employment prospects and personal safety, it should be treated as a civil rights violation.[86] Her idea of scaling penalties up based on the targets of the speech, in addition to the contents of the speech, is sensible. Such a legislative revision would take into account the realities of online harassment's effects on people who have historically suffered from hatred, bigotry and misogyny. The amplification effects of nonconsensual porn, which give harassers vastly more firepower as well as mobs of co-harassers, suggest that it is fair to increase penalties where the speech is directed at historically disempowered people.

These theoretical bases of liability may provide little relief in practice, however, if the victims cannot identify their attacker and if the victims feel unsafe themselves in asserting their claims. It is not easy to file a civil lawsuit asserting claims under any of these theories without disclosing the plaintiff's identity. The Federal Rules of Civil Procedure do not allow it presumptively; Rule 10(a) requires disclosure of the plaintiff's identity.[87] Many states have laws of procedure that mirror Rule 10(a).[88] A tradition in favor of open judicial proceedings, and therefore implicitly opposed to anonymous pleading, dates back to 15th century England.[89]

Filing a lawsuit under a false name requires judicial approval, and cannot be done as of right.[90] Every federal court requires judicial consent after consideration of several factors.[91] There is no uniform standard across circuits, however, and the standards for such consent vary considerably.

There is a strong judicial presumption that parties will use their real names in litigation, as required by Rule 10(a). One reason offered for this presumption is the idea that disclosing litigants' identities "furthers the public interest in knowing the facts surrounding judicial proceedings."[92] As another scholar put it, the right to proceed anonymously is disfavored because of the "shield and veil it creates

---

(last visited Jan. 16, 2018).

85. *Online Harassment & Cyberstalking*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/consumer-guides/online-harassment-cyberstalking (last visted Mar. 27, 2018)..

86. CITRON, HATE, *supra* note 55.

87. FED. R. CIV. P. 10(a) (requiring that all parties to a civil action be named in the complaint).

88. *See, e.g.*, ALASKA R. CIV. P. 10(a); ARK. R. CIV. P. 10(a); OHIO R. CIV. P. 10(a); S.C. R. CIV. P. 10(a).

89. David C. Scileppi, Note, *Anonymous Corporate Defamation Plaintiffs: Trampling the First Amendment or Protecting the Rights of Litigants?*, 54 FLA. L. REV. 333, 337–38 (2002).

90. Nat'l Ass'n of Waterfront Employers v. Chao, 587 F. Supp. 2d 90, 99 (D.D.C. 2008).

91. The legal standards are discussed in Section 0 *infra*.

92. *See, e.g., Nat'l Ass'n of Waterfront Employers*, 587 F. Supp. 2d at 99; *see also* Doe v. Vill. of Deerfield, 819 F.3d 372, 376–77 (7th Cir. 2016) (stating that the public has a right to know the names of litigants who take up time, space, and money in the court system that the public is paying for).

between the court and the public."[93] Some courts justify the requirements of Rule 10(a) by reference to the public's interest in open trials because it requires plaintiffs to "name all the parties."[94] While the Supreme Court has acknowledged that there are circumstances in which the general interest in judicial openness is outweighed by other interests, it has noted that those instances are rare.[95]

In response, however, some scholars have pointed out that the public interest in open trials is not undermined by allowing plaintiffs to proceed under a pseudonym. As Professor Kessler observed, "[i]t is the rare case today in which the public cannot realize the full benefits of an open trial without knowing the plaintiff's name" because salient elements of the plaintiff's identity are widely available through electronic databases.[96] Professor Edwards has also suggested that pseudonymous proceedings actually may make trials fairer because it is less likely in those cases that the jurors will be able to search the internet for, and be influenced by, information that is not presented at trial.[97]

In certain types of cases, however, more leeway is granted to plaintiffs who want to proceed anonymously.[98] Courts usually grant requests to proceed anonymously to victims in cases involving sexual assault.[99] Anonymity is also often granted in cases involving minors.[100]

---

93. Chloe Booth, *Good Things Don't Come to Those Forced to Wait: Denial of a Litigant's Request to Proceed Anonymously Can be Appealed Prior to Final Judgment in the Wake of* Doe v. Village of Deerfield, 58 B.C.L. Rev. E. Supp. 205, 211–12 (2017).

94. FED. R. CIV. P. 10(a); *see* Doe v. Del Rio, 241 F.R.D. 154, 156 (S.D.N.Y. 2006) (stating that Rule 10(a) "has constitutional overtones" related to the public interest in open proceedings). But Professor Carol M. Rice disputes whether Rule 10(a) has any direct connection to the policy goals advanced by open judicial proceedings. She argues that Rule 10(a)'s pleading requirements are not designed to preserve open courts or to bar pseudonymous pleading, and contends that "Rule 10(a) simply seeks to distinguish the more formal caption in the complaint from all others, which for economy need not list every party," and that "Rule 10(a) does not necessarily dictate the substance of the name designation."
Carol M. Rice, *Meet John Doe: It Is Time for Federal Civil Procedure to Recognize John Doe Parties, 57* U. PITT. L. REV. 883, 915 (1996).

95. *See* Globe Newspaper Co. v. Superior Ct. for Norfolk Cty., 457 U.S. 596, 606 (1982) (stating that the circumstances under which proceedings in a criminal trial should not be shared with the public are limited).

96. Jayne Kessler, *Privacy, Plaintiff, and Pseudonyms: The Anonymous Doe Plaintiff in the Information Age*, 53 KANSAS L. REV. 195, 218 (2004).

97. Edwards, *supra* note 7, at 445.

98. *See* Doe v. Blue Cross & Blue Shield United of Wis., 112 F.3d 869, 872 (7th Cir. 1997) (giving examples of types of cases, such as those that require privacy protections for rape victims and other vulnerable parties, that warrant a party to a litigation to proceed anonymously); Doe v. City of Chicago, 360 F.3d 667, 669 (7th Cir. 2004) (adding that a party's fear of retaliation as a response for instituting a litigation can be a compelling reason for the court to allow the party to proceed anonymously).

99. *See, e.g.*, Roe v. Borup, 500 F. Supp. 127, 130 (E.D. Wis. 1980) (allowing anonymity in a case involving false claims of child sexual abuse to curb plaintiff's future psychological harm); Doe v. Howe, 607 S.E.2d 354, 357 (S.C. Ct. App. 2004) (allowing plaintiff who was sexually abused by a school employee to use a pseudonym).

100. *See, e.g.*, Doe v. Stegall, 653 F.2d 180, 186 (5th Cir. 1981) (allowing anonymity for plaintiffs who challenged constitutionality of prayer and bible readings in a public school because of real threatened violence and retaliation against their children); *see also* Lisa M. Jones et al., *Protecting*

Following this presumption, courts generally permit pseudonymous litigation "only in those exceptional cases involving matters of a highly sensitive and personal nature, real danger of physical harm, or where the injury litigated against would be incurred as a result of the disclosure of the plaintiff's identity."[101] Using a false name is not allowed "where the plaintiff merely cites personal embarrassment" as the reason for seeking confidentiality.[102]

Aside from these types of cases, courts usually engage in balancing tests to determine whether to approve a plaintiff's request to file under a false name.[103] There is no uniform federal standard as to when this approval should be given. The D.C. Circuit Court follows the five factor test set out in *National Association of Waterfront Employers v. Chao*, which directs courts to consider:[104]

> "(1) whether the justification asserted by the requesting party is merely to avoid the annoyance and criticism that may attend any litigation or is to preserve privacy in a matter of a sensitive and highly personal nature; (2) whether identification poses a risk of retaliatory physical or mental harm to the requesting party or even more critically, to innocent non-parties; (3) the ages of the persons whose privacy interests are sought to be protected; (4) whether the action is against a governmental or private party; and (5) the risk of unfairness to the opposing party from allowing an action against it to proceed anonymously."[105]

The factors that provide the most room for debate in this context are the first and second. The first, which asks whether the request is "merely" to avoid annoyance or to "preserve privacy in a matter of a sensitive and highly personal nature," will swing in the plaintiff's favor if the court agrees that the online harassment is, in fact, sensitive and highly personal. It is easy to imagine a judge finding that the nonconsensual spread of nude photographs initially taken with the plaintiff's consent is neither sensitive nor highly personal. Many people still blame the victims of nonconsensual pornography. While rape shield laws protect rape victims from having evidence of prior consensual sex with the defendant used as evidence against them, there are no comparable protections for victims of nonconsensual pornography.

The second factor considers the risk of "retaliatory physical or mental harm" to the plaintiff and to "innocent non-parties." The risk of mental harm likely will be more significant than the risk of physical harm to most victims of online

---

Victims' Identities in Press Coverage of Child Victimization, 11 JOURNALISM 347, 349 (2010) (explaining that enhanced privacy provisions for minors in the judicial system stems from the idea that stigma is especially detrimental to a child's development and impedes the child's ability to move on from bad circumstances in their past).

101. Nat'l Ass'n. of Waterfront Employers v. Chao, 587 F. Supp. 2d 90, 99–100 (D.D.C. 2008) (quotations omitted)..

102. *Id.*at 100.

103. *See Stegall*, 653 F.2d at 186 (announcing that there is no "hard and fast formula" in deciding when a party may proceed anonymously but the decision calls for a balancing of the parties' interests); Booth, *supra* note 93, at 213 (explaining that courts routinely balance a number of factors in weighing the parties' interests); *see also* Edwards, *supra* note 7 at 441 (explaining that the procedural methods for proceeding pseudonymously vary by circuit).

104. *Nat'l Ass'n of Waterfront Employers*, 587 F. Supp. 2d at 99.

105. *Id.*

harassment. Some victims have experienced physical harm from their online stalkers, however, and a United Nations study has suggested that cyber violence is equivalent to physical violence for women.[106] To the extent that the risk of "mental harm" requires expert testimony from a mental health professional, however, that determination only increases the cost and decreases the accessibility of this option for putative plaintiffs.

The third factor, concerning the age of the person whose privacy would be protected, does not limit relief to minors by its terms. It does suggest, however, that the court is more likely to grant relief to younger applicants.

Whether a nonconsensual porn victim would be able to satisfy each of these factors depends on at least two considerations. The first is whether the victim will be able to establish that the request is justified in order to "preserve privacy in a matter of a sensitive and highly personal nature," as the first factor states. The private and personal nature of nonconsensual porn makes it likely that this factor will weigh in favor of the victim.

The second consideration is whether the judge evaluating the request takes a conservative or progressive view of the alleged nonconsensual porn and its accompanying damages. In other words, is the judge more likely to see the nonconsensual disclosure and reposting of sexual images as posing a "risk of retaliatory … mental harm to the requesting party" or as "mere" personal embarrassment? The former would weigh in favor of allowing the pseudonymity, while the latter would weigh against it. There is reason to believe that at least some judges will take a more conservative view. In one recent analysis of judicial language in revenge porn cases, a scholar observed that courts rely on what she calls "trivializing words" to downplay or minimize the kinds of harm that the victims experienced.[107] "In these opinions," she notes, "judicial language generally indicates little to no recognition of the harms that the victim experienced or of the impacts of the amplification effects of revenge porn."[108]

The consequences of denying a putative plaintiff's motion to proceed anonymously can be significant. Without this option, and in the face of the public humiliation, shame and fear of retaliation, such plaintiffs are likely to abandon their claims.[109] One scholar has suggested that compelling plaintiffs who alleged sexual crimes to litigate under their real names is a form of re-victimization.[110] As the ability to collect personal details about people through internet searches expands, including those people's addresses and employers, the potential backlash against plaintiffs in nonconsensual porn cases may become more severe.

106. Charlotte Alter, *U.N. Says Cyber Violence Is Equivalent to Physical Violence Against Women*, TIME (Sep. 25, 2015) http://time.com/4049106/un-cyber-violence-physical-violence/.

107. Vora, *supra* note 24, at 243.

108. *Id.* at 245.

109. Booth, *supra* note 93, at 218.

110. Andrea A. Curcio, *Rule 412 Laid Bare: A Procedural Rule That Cannot Adequately Protect Sexual Harassment Plaintiffs from Embarrassing Exposure*, 67 U. CIN. L. REV. 125, 155–56 (1998) (explaining that childhood sexual abuse is one of the most personal and private issues and forcing a plaintiff to have this abusive past exposed has the potential to be irreparably damaging).

C. State Regulation of Nonconsensual Porn Provides Inconsistent Relief and Insufficient Victim Anonymity

The difficulties posed by inconsistent anonymity pleading standards have not been resolved by the recent explosion of new nonconsensual porn regulation at the state and local levels. These new laws prohibiting nonconsensual pornography is a vital component of the legal response to this problem. Without a clear means of unmasking potential defendants, however, these legislative efforts are ineffective in many cases and perhaps in the most severe cases. In addition, these cases can be hard to litigate for procedural reasons. The police may be unfamiliar with the state laws, if any, or may be unsure about how to establish the computer forensics necessary to prosecute the case.[111]

Perhaps in response to the insufficiency of traditional tort remedies to combat nonconsensual porn, states and some cities have stepped in to create new nonconsensual porn legislation. In November 2017, New York City passed its own nonconsensual porn law, as New York State does not yet have a similar law.[112] New York City's law makes the nonconsensual dissemination of intimate images "with the intent to cause economic, physical or substantial emotional harm" a misdemeanor, punishable by a $1,000 fine and up to one year of jail.[113] While celebrating this development, Mary Anne Franks, a leading scholar of nonconsensual porn regulation and co-founder of the Cyber Civil Rights Initiative, noted that the likely effectiveness of the law was limited in three ways.[114] First, the intent requirement narrows the scope of the crime to revenge porn, letting people who engage in nonconsensual porn for "profit or entertainment purposes completely off the hook."[115] Second, the law contains an exception for disclosures protected by the First Amendment, and it is not clear what that means in this context. Finally, Franks noted that the classification of revenge porn as a misdemeanor limits the extent to which prosecutors will investigate and pursue these cases seriously.[116]

The rapid expansion of state revenge porn laws, from 3 in 2012 to 38 in 2017, attests to the viral spread of nonconsensual porn and the need for a unique regulatory approach. Until 2012, only three states – New Jersey, Alaska and Texas – had outlawed nonconsensual pornography. Since 2012, however, 35 other states have outlawed this conduct.[117] The distribution of sexually explicit images without the subject's consent therefore is now illegal under the laws of 38 states as well as

---

111. Margaret Talbot, *Taking Trolls to Court*, at 56 NEW YORKER, Dec. 15, 2016.

112. Melanie Ehrenkranz, *Revenge Porn is Finally Criminalized in New York City*, GIZMODO (Nov. 16, 2017) https://gizmodo.com/revenge-porn-is-finally-criminalized-in-new-york-city-1820482756.

113. *Id.*

114. *Id.*

115. *Id.*

116. *Id.*

117. These include Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Minnesota, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, North Dakota, Oklahoma, Oregon, Pennsylvania, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia and Wisconsin. *38 States + DC Have Revenge Porn Laws*, CYBER CIVIL RIGHTS INITIATIVE, https://www.cybercivilrights.org/revenge-porn-laws/ (last visited Jan. 19, 2018).

the District of Columbia.[118] These laws vary tremendously in their content and scope.[119] In addition, legislative efforts to enact similar laws are underway or are pending in eight other states as well as Puerto Rico.[120]

There is no federal law against nonconsensual pornography in the United States. A Senate proposal to criminalize nonconsensual porn, whose short title is the Ending Nonconsensual Online User Graphic Harassment (ENOUGH) Act of 2017, was introduced in November 2017.[121] Facebook and Twitter supported the bill.[122] The previous year, in August 2016, Representative Jackie Speier introduced a similar bill called the Intimate Privacy Protection Act that would have established a federal law prohibiting its distribution.[123] The bill was not enacted.[124]

The regulation of nonconsensual porn is challenging in part because of First Amendment concerns. Laws restricting the content of speech, possibly including nonconsensual pornography, are invalid for violation of the First Amendment unless they are "necessary to a compelling state interest."[125] Courts have, however, allowed the proscription of many kinds of harmful speech, including incitement, threats, obscenity, child pornography and criminal conspiracies.[126] Laws targeting nonconsensual porn may risk a First Amendment challenge because of their presumed content-based restrictions.[127] As Professor Mary Anne Franks explained in a guide to developing effective revenge porn laws, laws that criminalize behavior based on an intent to harass, humiliate or cause emotional distress may also violate the First Amendment by characterizing that behavior as harassment rather than an invasion of privacy.[128] One scholar has suggested that nonconsensual porn may be regulated as a form of hate speech or group libel, which has low First Amendment value.[129] Unlike group libel, which is less protected because it undermines social beliefs about a portion of the population[130], however, nonconsensual porn is almost always directed at an individual.

---

118. *Id.*

119. *See id.*

120. Franks, *supra* note 22, at 4.

121. Ending Nonconsensual Online User Graphic Harassment (ENOUGH) Act of 2017, S. 2162, 115th Cong. (2017).

122. Chris Morris, *Revenge Porn Law Could Make It A Federal Crime to Post Explicit Photos Without Permission,*
FORTUNE (Nov. 28, 2017), http://fortune.com/2017/11/28/revenge-porn-law/.

123. Intimate Privacy Protection Act of 2016, H.R. 5896, 114th Cong. (2016).

124. *Id.*

125. Koppelman, *supra* note 51, at 662.

126. *Id*.

127. Cooke, *supra* note 52, at 482.

128. Franks, *supra* note 22, at 7, 8.

129. Cooke, *supra* note52, at 485.

130. GEOFFREY R. STONE ET AL., THE FIRST AMENDMENT 258 (5th ed. 2016) ("Group libel is of 'low' First Amendment value because it operates not by persuasion but by insidiously undermining social attitudes and beliefs.").

One advocacy organization dedicated to ending nonconsensual porn[131], the Cyber Civil Rights Initiative, has developed model state[132] and federal[133] criminal laws as well as a model civil law[134] to combat nonconsensual porn. The model civil law provides an option for proceeding anonymously, specifying that "all information about the plaintiff may be redacted from pleadings and court filings and the plaintiff may proceed under [a] pseudonym."[135] It also mandates that the "court shall inform the plaintiff of the option to proceed under [a] pseudonym at the earliest possible point and shall maintain the records in a manner that protects the plaintiff's confidentiality."[136] These provisions underscore the importance, from the perspective of advocates for effective nonconsensual porn legislation, of allowing plaintiffs to proceed without fear that their personal information will be disclosed to the public as a consequence of litigation. The model civil law does not, however, make any provision for uncovering the identity of a pseudonymous defendant.

Indeed, only a few enacted state laws allow nonconsensual porn victims to proceed anonymously. Under Connecticut's recently revised laws, the names and addresses of victims of "voyeurism" (as the state describes the crime of recording another person without that person's knowledge and consent) are confidential.[137] The victim's identifying information may only be disclosed by order of the state's Superior Court, although the information may be provided to the accused.[138] Victims of voyeurism also need not disclose their address or telephone number during any trial or evidentiary hearing, which further reduces the risk that their contact information will be disclosed on official court transcripts.[139]

While these provisions are admirable, their benefits are limited by the relatively narrow scope of the statute. Connecticut's definition of "voyeurism" omits much of what is popularly understood as nonconsensual porn. For example, "voyeurism" is defined as knowingly recording images of another person without that person's knowledge and consent when the subject has a reasonable expectation of privacy under any of the following conditions: (1) with malice, (2) for sexual gratification, (3) by trespass or (4) when the images are of the other

131. While the Cyber Civil Rights Initiative's website notes that its initial campaign was to end "revenge porn," its "Guide for Legislators" explains that the term "'revenge porn,' though popular, is misleading" and notes that '[m]any victim advocates . . . use the term "nonconsensual pornography." *Compare The End Revenge Porn (ERP) Campaign*, CYBER CIVIL RIGHTS INITIATIVE, https://www.cybercivilrights.org/erp-campaign/ (last visited Jan. 16, 2018) *with Guide for Legislators*, CYBER CIVIL RIGHTS INITIATIVE, https://www.cybercivilrights.org/guide-to-legislation/ (last visited Jan. 16, 2018).

132. *CCRI Model State Law*, CYBER CIVIL RIGHTS INITIATIVE, https://www.cybercivilrights.org/model-state-law/ (last visited Jan. 16, 2018).

133. *CCRI Model Federal Law*, CYBER CIVIL RIGHTS INITIATIVE, https://www.cybercivilrights.org/ccri-model-federal-law/ (last visted Mar. 27, 2018).

134. *CCRI Model Civil Law*, CYBER CIVIL RIGHTS INITIATIVE, https://www.cybercivilrights.org/ccri-model-civil-law/ (last visited Mar. 27, 2018).

135. *Id*.

136. *Id*.

137. An Act Concerning Invasions of Privacy, 2015 Conn. Pub. Act No. 15-213, 4-5 (Reg. Sess.).

138. *Id*.

139. *Id*.

person's genitals or buttocks (which presumably covers "upskirting").[140] In effect, "voyeurism" as defined here applies only to nonconsensual recording, and not to nonconsensual distribution. It does not regulate the nonconsensual distribution of images taken with the subject's consent even when there is an expectation that those images will remain private. A woman who sends nude pictures voluntarily by text to her boyfriend would have no cause of action under Connecticut's laws if that boyfriend then posted those private images to a website or on social media.

California's nonconsensual porn laws establish a kind of de facto mens rea of intent to cause "serious emotional distress." They provide, *inter alia*, that when a person distributes intimate images of another "under circumstances in which the persons agree or understand that the image shall remain private," the distributor "knows or should know that distribution of the image will cause serious emotional distress, and the person depicted suffers that distress."[141]

D. Minnesota's Law Illustrates the Need for Greater Victim Protections.

In 2016, Minnesota passed the most comprehensive state revenge porn law yet, but even this law does too little to support victims and encourage them to come forward. This law, which went into effect on August 1, 2016, created both civil and criminal penalties by making it unlawful to "disseminate private sexual images of another without consent."[142] The law also prohibits sexual solicitation without the subject's consent,[143] such as in cases where a defendant posts a plaintiff's personal information on a website such as Craigslist and, without her consent, invites other people to contact her for sex. It creates a civil cause of action, allowing the court to award a prevailing plaintiff general and special damages, as well as any profit made from the dissemination of the images.[144] In addition, the court may award a civil penalty to the plaintiff, up to $10,000, as well as court costs and reasonable attorneys' fees.[145] There is also a provision for injunctive relief, with a civil fine of up to $1,000 per day for failure to comply with the injunction.[146] This would penalize the continued display and/or distribution of the nonconsensual images.

The exclusions in the Minnesota law are as important as its inclusions. It explicitly excludes from coverage images made for the purpose of the legal sale of goods, including the "creation of artistic products for sale or display."[147] It also contains an exception for images that "relate to a matter of public interest" where "dissemination serves a lawful purpose."[148] The latter exception provides cover for

140. *Id.*

141. California S.B. 1255, Sec. 1.7 (amending Penal Code Section 647(j)(4)(A).

142. Memorandum from Chris Turner, Minnesota Senate Fiscal Analyst, "S.F. No. 2713 - Dissemination of Private Sexual Images; Civil Action and Criminal Penalties (First Engrossment)" (May 2, 2016), http://www.senate.leg.state.mn.us/departments/scr/billsumm/summary_display_from_db.php?ls=89&id=4659.

143. Revenge Pornography Act, MINN. STAT. § 604.31(2) (2016).

144. *Id*. at § 604.31(3)

145. *Id.*

146. *Id*. at § 604.31(4)

147. *Id*. at. § 604.31(6)(a)(4).

148. *Id*. at § 604.31(6)(a)(5).

journalists who post sex tapes of celebrities, for example, if they can establish that it is in the public interest to do so. Another interesting feature of the Minnesota's revenge porn law is its recognition of the need for sensitivity toward the privacy of the plaintiff. To this end, the law specifically allows for the confidentiality of filings under the statute "to protect the privacy of the plaintiff."[149]

Recent litigation under this statute, however, demonstrates the shortcomings of this law. In a recent case, the Minnesota Court of Appeals affirmed the district court's denial of the plaintiff's request to proceed as "Jane Doe" in a lawsuit involving the nonconsensual filming of her while she was partially nude.[150] The appellant, a professional entertainer, was hired to perform at a show involving a Hawaiian dance for a client company.[151] Alleging that the defendants allowed their security cameras to capture her image while she was changing costumes, she sued them for negligence, invasion of privacy, and intentional and negligent infliction of emotional distress.[152] In her complaint, she used a Jane Doe pseudonym, explaining that "she wished to proceed under a pseudonym because of the risk of harm to her career, reputation, and relationships if it were public knowledge that she had been filmed while partially nude."[153] The District Court denied her request, explaining that the Rules of Civil Procedure required her to use her true name and declining to exercise its discretion to allow her to proceed under a pseudonym.[154] It reasoned that "the public's interest in an open and transparent judiciary outweighed appellant's claimed privacy interest."[155]

On appeal, Doe argued that the district court abused its discretion by failing to take into account factors recognized by other courts favoring pseudonymity.[156] She also challenged the court's characterization of her privacy interest as "changing clothes."[157] The appellate court noted that while the state's civil procedure rules mandate that a party must include her true name on the summons and complaint, some statutes permit pseudonymous pleading.[158] It expressly recognized that the newly enacted Minnesota nonconsensual porn law "expressly requires district courts to allow confidential filings in cases brought under the statute in order to protect the plaintiff's privacy."[159] However, because the appellant did not frame her original claims as a violation of that statute, the court summarily concluded that its exceptions did not apply to her claims.[160]

---

149. *Id.* at § 604.31(5) (2016).

150. Doe v. Empire Ent., LLC, No. A16-1283, 2017 Minn. App. Unpub. LEXIS 419, at *1–2 (Minn. Ct. App. May 8, 2017).

151. *Id.* at *2.

152. *Id.*

153. *Id.*

154. *Empire Ent., LLC*, 2017 Minn. App. Unpub. LEXIS 419, at *3.

155. *Id.*

156. *Id.*

157. *Id.* at *3–4.

158. *Id.* at *5–6.

159. *Id.*

160. *Id.* While the decision does not explain why Doe did not assert claims under Minnesota's NCP statute, one possibility is that the statute did not go into effect in time. The events Doe alleged in her complaint took place in January 2016, and Minnesota's law did not go into effect until August 1, 2016. Alternatively, it may have been an oversight on the part of her attorney, Peter Nickitas, who has been

In response to appellant's arguments that the court should have evaluated her request according to factors used by other federal courts, the appellate court noted that Minnesota has not adopted a test for district courts to use when considering a request for pseudonymous pleading.[161] It observed that most federal courts of appeal have established a balancing test in such cases, although the circuits differ on the factors to be weighed.[162] While the language of the Federal Rules of Civil Procedure is identical to that of the Minnesota rules on naming parties, Minnesota appellate courts are "not bound by federal interpretations of the federal rule."[163]

If there were an exception to the Minnesota rules, the court noted, it would be the province of the Minnesota Supreme Court and the "statutory rule-making process" to create one.[164] It then concluded that the district court did not abuse its discretion by determining that the public interest in open proceedings outweighed the plaintiff's interest in privacy.[165] In dictum, the court suggested that this debate could have been avoided if the defendants had been more civil, noting that a defendant's decision to challenge a plaintiff's request to proceed anonymously when "facing claims of a highly sensitive nature . . . could be viewed in some quarters and in some cases as unseemly."[166]

What is missing from the appellate court's analysis is a response to the appellant's claims that the district court unfairly minimized her privacy interest. While the court emphasized the traditional legal preference for open proceedings, nowhere in the decision did it analyze the weight of the countervailing interest in privacy in claims "of a highly sensitive nature." It did not extrapolate an interest in procedural privacy from the statutory permission to file pseudonymously granted by the state's new nonconsensual porn law, which appears to cover harms similar to those asserted by the appellant. Nor did it evaluate, even briefly, the appellant's claims that she would suffer personal and professional harm from the use of her true name in the proceedings. It is easy to determine that the public's interest in open proceedings outweighs a complainant's interest in privacy when there is no acknowledgment of the severity of the harms that may flow from violation of that privacy in the instant case. *Doe v. Empire* illustrates the limitations of even a model state nonconsensual porn law when it comes to the privacy interests of nonconsensual porn victims.

E. The Standards for Doe Plaintiffs Should Be Revised Fairly

Given the extreme and permanent damage that nonconsensual porn can cause in this age of amplification, and the insufficient protections provided by

---

suspended from practice in Minnesota four times as of this writing. *See* Seth Leventhal, *Peter "Extreme Caution" Nickitas Strikes Again, Gets a Spare This Time*, MINNESOTA LITIGATOR (Aug. 18, 2017) http://www.leventhalpllc.com/2017/08/peter-extreme-caution-nickitas-strikes-again-gets-a-spare-this-time/.

161. *Empire Ent., LLC*, 2017 Minn. App. Unpub. LEXIS 419, at *7.

162. *Id.* at *8–9 (citing Doe v. Megless, 654 F.3d 404, 410 (3d. Cir. 2011)).

163. *Empire Ent., LLC*, 2017 Minn. App. Unpub. LEXIS 419, at *8.

164. *Id.* at *10.

165. *Id.* at *10–11.

166. *Id.* at n 3.

nonconsensual porn laws in most states, it should be easier for plaintiffs to sue anonymously in online harassment cases where they can demonstrate that suing under their real name will increase the likelihood of mental harm. Even if it were easier for plaintiffs to file anonymous lawsuits against their online harassers, there would still be considerable barriers to justice for many plaintiffs. The cost of private litigation remains prohibitive, and the procedural work involved in securing the right to sue anonymously would only add to that cost.

III. REVENGE PORN DEFENDANTS RECEIVE TOO MUCH IDENTITY PROTECTION

Should courts adopt a prima facie standard to enable these victims to unmask anonymous commenters more easily? If there is a right to speak anonymously on the internet, that right may be outweighed by the rights of tort victims to bring alleged anonymous harassers to justice. Although making it easier for victims of online harassment to discover the identities of their harassers may be an attractive remedy, the practical and ethical difficulties of unmasking anonymous harassers are substantial.

In some cases, the anonymous perpetrators and promoters of nonconsensual porn can be identified by the ICPs that host them. In many cases, however, even the internet service providers (ISPs) and ICPs do not know the posters' real identities and therefore cannot disclose them, as described below. Even when ISPs and ICPs know these real identities, there is little legal incentive for them to disclose those identities because they are shielded from liability for the postings by the CDA.[167]

Because not all anonymous posters can be unmasked, there is a strong need for greater deterrence of nonconsensual porn at the ICP level. ICPs should be compelled to monitor, deter and otherwise minimize the harm caused by nonconsensual porn because they are in the best technological position to do so. The fact that they are able to do so is evident from the voluntary efforts some ICPs are beginning to make under public pressure. While these voluntary efforts are laudable, there would be greater security for nonconsensual porn victims if such efforts were legally required and widely applicable to all ICPs, including those who have not yet chosen to engage in them.

A. Anonymity Exacerbates Online Harassment

It has never been easier to be anonymous online. As it has become easier to track and monitor people's internet usage, and as public awareness of monitoring has increased, new resources have sprung up to make it easier to use the internet anonymously. One example is Tor, an anonymizing browser.[168] Tor describes itself as "an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security."[169] It is unlikely that internet users will give up their anonymity online in the future.

---

167. Communications Decency Act of 1996, 47 U.S.C. §230 (c)(1) (1996).

168. TOR, https://www.torproject.org/ (last visited Jan. 19, 2018).

169. *Id.*

In recent years, scholars have debated the extent to which anonymity should be regulated on the Internet, especially in the context of tort and obscenity allegations.[170] This is an especially contentious issue with regard to nonconsensual porn because anonymity is a significant factor in nonconsensual porn and online harassment in general. In many cases, online threats come from anonymous sources. More than half of those who have experienced online harassment say that they did not know the person involved in the most recent harassing incident.[171] The internet itself facilitates anonymity, by enabling people to post under assumed names. [172] More than 60% of internet users believe that online environments allow for more anonymity than their offline lives do.[173] This belief is well grounded. Facebook found that harassment, bullying, and other online abuse is committed by people using fake names eight times more often than by people using their real names.[174]

Yet anonymity online has important benefits. There is an honorable tradition of speaking anonymously or pseudonymously, especially about controversial issues. Most of the Federalist Papers were first published under pseudonyms, including those penned by Alexander Hamilton.[175] Anonymity promotes free expression by minimizing the risks attached to being identified with specific beliefs or practices. It protects individuals' privacy from public and private tracking. In a conservative political environment, for example, liberal thinkers may be more interested in hiding their search activity from potential monitoring because they anticipate the possibility of negative repercussions in the future. Being anonymous online can also have more vital consequences. For certain groups, such as many victims of domestic violence whose abusers may seek them and their children out, anonymity is essential to everyday safety and wellbeing. For example, domestic violence victims benefit from the ability to be able to rebuild their lives without the risk of being located by their abusers. It would be not only unwise, but also dangerous to get rid of online anonymity altogether.

B. Anonymous Nonconsensual Porn Perpetrators Cannot Be Unmasked Easily

The spate of new state laws creating civil and criminal penalties for nonconsensual porn does little to help victims of anonymous nonconsensual porn

---

170. *See, e.g.*, Bryan H. Choi, *The Anonymous Internet*, 72 MD. L. REV 501 (2013) (suggesting that internet regulators limit anonymity to avert more onerous limitations on generativity); Victoria Smith Ekstrand, *Unmasking Jane and John Doe: Online Anonymity and the First Amendment*, 8 COMM. L & POL'Y 405 (2003); Jason M. Shepard & Genelle Belmas, *Anonymity, Disclosure and First Amendment Balancing in the Internet Era: Developments in Libel, Copyright, and Election Speech*, 15 YALE J.L. & TECH. 92 (2012–13) (recommending adoption of a prima facie standard to unmask online speakers); Sophia Qasir, Note, *Anonymity in Cyberspace: Judicial and Legislative Regulations*, 81 FORDHAM L. REV. 3651 (2013) (suggesting that courts expand the remedies available to victims of harmful online speech and proposing a summary judgment standard for unmasking online speakers).

171. Duggan, *supra* note 37.

172. *Id*.

173. *Id.*

174. Lisa Vaas, *Facebook Finally Changes Real-Name Policy*, NAKED SECURITY (Nov. 3, 2015) https://nakedsecurity.sophos.com/2015/11/03/facebook-finally-changes-real-name-policy/.

175. Chesa Boudin, Note, *Publius and the Petition:* Doe v. Reed *and the History of Anonymous Speech*, 120 YALE L.J. 2140, 2153 (2010-2011).

posts if neither the victim nor law enforcement officials can identify the perpetrators. Plaintiffs must be able to identify defendants to sue them. When a victim of nonconsensual porn discovers that her images have been shared on the internet, she may not know the true identity of the person or people who shared the images. In such cases, a primary obstacle for potential plaintiffs in addressing these torts is finding out who the speaker is. Many harassers do not post under their own name, preferring to hide behind a pseudonymous user name. This is a common practice. It is easier for people to post potentially offensive comments and images under false names than under their own because there is less accountability for doing so.[176]

While anonymity makes it easier to post nonconsensual porn images, it is harder for victims of nonconsensual porn to bring anonymous posters to justice in a civil action. Because courts have recognized a qualified right to speak anonymously,[177] there is no simple way to unmask an anonymous commentator. The Ninth Circuit has held that there is a Constitutional right to speak anonymously without clarifying the standards under which an anonymous speaker may exercise that right.[178] It has clarified, however, that whenever a party seeks the identity of an anonymous online poster, "the nature of the speech should be a driving force in choosing a standard."[179] It also mandates that the Court "consider[] the important value of anonymous speech balanced against a party's need for relevant discovery in a civil action."[180] Virginia is the only state that has passed legislation defining the standards that must be met before an anonymous speaker's identity can be disclosed to a requesting party.[181] California considered similar legislation but did not pass it.[182]

Over the last two decades, federal courts and some state courts have adopted rules for unmasking unknown defendants who are accused of committing certain torts online, including defamation, intellectual property infringement, tortious interference with contractual relations, and fraud.[183] In such instances, the plaintiff is required to make some showing of likelihood of success beyond the standard pleading requirements.[184] However, the difficulties plaintiffs face in making such

176. Duggan, *supra* note 37.

177. Mallory Allen, *Ninth Circuit Unmasks Anonymous Internet Users and Lowers the Bar for Disclosure of Online Speakers*, 7 WASH. J.L. TECH. & ARTS 75, 76-77 (2011).

178. *Compare with* In re Anonymous Online Speakers, 661 F.3d 1168, 1177 (9th Cir. 2011) (refusing to hold that district court abused its discretion in applying a summary judgment standard) *with* S103 Inc. v. Bodybuilding.com LLC, 441 F. Appx. 431, 433 (9th Cir. 2011) (vacating the district court's decision to use a summary judgment standard); *see also* OBI Pharma, Inc. v. Does 1-20, Order Granting Ex Parte Motion for Early Discovery (S.D. Cal. 2017) (acknowledging that "The Ninth Circuit has not identified one specific test that applies anytime [sic] a party seeks the identity of an anonymous online poster through discovery.").

179. *OBI Pharma, Inc.*, Order Granting Ex Parte Motion for Early Discovery (S.D. Cal. 2017).

180. *Id.* (citing *In Re Anonymous Online Speakers*, 661 F.3d at 1176).

181. *See* VA. CODE ANN. §8.01-407.1 (2012).

182. A.B. 1143, 2003 Leg., Reg. Sess. (Cal. 2003), available at ftp://www.leginfo.ca.gov/pub/03-04/bill/asm/ab_1101-1150/ab_1143_bill_20030430_amended_asm.html.

183. See Marian K. Riedy; Kim Sperduto, *Revisiting the Anonymous Speaker Privilege*, 14 N.C. J.L. & TECH. 249, 250 (2012).

184. Reno v. ACLU, 521 U.S. 844, 870 (1997); Amy P. Nickerson, Comment, *Coercive Discovery and*

a showing have been subject to critical consideration, and scholars have begun to question the wisdom of protecting anonymous posters online.[185] Some have pointed out that anonymity online is especially dangerous, rather than being worthy of special protection.[186] Professors Reidy and Sperduto argue that "the anonymous speaker privilege needs a substantial redirection not only because of the shaky jurisprudential basis for the privilege as it has been constructed, but also because the policy considerations that originally justified the creation of the privilege have been undermined by the realities of today's Internet."[187] Despite substantial criticism of the anonymous speaker privilege among legal scholars, it largely remains in place.

If unmasking anonymous posters is challenging in a civil case, the criminal law alternative may be even worse. The criminal justice system is especially daunting for victims who cannot identify a defendant. Someone whose nonconsensual porn images are posted anonymously will have more difficulty getting criminal charges filed on her behalf than she would if the speaker were known. Law enforcement officials may be unmotivated to try to identify anonymous speakers, in part because doing so is expensive and time-consuming. Identification may require the use of computer forensic specialists, which may require cooperation with outside agencies.[188] Although one scholar has proposed a model federal cyber-harassment statute that would provide incentives for the investigation of anonymous online harassers, no such incentive currently exists.[189]

C. ICPs Should Unmask Anonymous Posters, Subject to Limitations

When it is possible to discover the identity of an anonymous nonconsensual porn poster by asking the hosting ICP, a victim or prosecutor may make that request. The most direct way to discover the identity of an anonymous poster is to compel the ICP hosting the speaker to disclose his identity. This is likely to yield mixed results, in that ICPs are notoriously resistant to such pressure. The mechanism for doing so may include issuing a subpoena to the ICP, with a substantial penalty attached for noncompliance. ICPs are unlikely to provide this information voluntarily. Google, for example, specifies only one court from which is accepts requests from user data, and notes that "requests to identify users by real names or IP addresses may be declined."[190]

---

the First Amendment: Towards a Heightened Discoverability Standard, 57 UCLA L. REV. 841, 846 (2010).

185. Michael S. Vogel, *Unmasking "John Doe" Defendants: The Case Against Excessive Hand-Wringing Over Legal Standards*, 83 Or. L. Rev. 795, 822 (2004) ("The general right to speak anonymously on the Internet is substantially different from the asserted right to remain anonymous when anonymity is being used as a shield protecting tortious or illegal conduct. The rapidity with which false information, trade secrets, and the like can be spread over the Internet creates a serious hazard, a hazard which must be weighed in determining the proper judicial approach to these situations.").

186. Danielle Keats Citron, *Cyber Civil Rights,* 89 B.U. L. REV. 61, 63 (2009).

187. Reidy and Sperduto, *supra* note 183, at 253.

188. A. Meena Seralathan, *Making the Time Fit the Crime: Clearly Defining Online Harassment Crimes and Providing Incentives for Investigating Online Threats in the Digital Age*, 42 BROOKLYN J. INT'L L. 425, 429 (2016).

189. *Id.*

190. *Serving Civil Subpoenas or Other Civil Requests on Google*, GOOGLE, https://support. google.com/faqs/answer/6151275?hl=en1497538752037 (last visited Jan. 19, 2018).

Another problem with such subpoenas is that many ICPs cannot comply because they lack the knowledge to do so. ICPs may not even know the real identity of any particular user. While Facebook requires users to use their real names,[191] other ICPs and ISPs do not. Google discontinued its real name policy in 2014, after three years of intense debate over the wisdom of controlling users' ability to define their own online identity.[192] Ongoing conflicts over policies that require users to disclose their real names are sometimes referred to as the "nymwars," derived in part from the suffix "-nym" (as in pseudonym.)[193]

In many other cases, however, it is possible for the ICP to identify the name of the poster. Social media companies may choose to comply with subpoenas. Doing so in the case of an accused nonconsensual porn poster certainly would be consistent with these companies' use policies prohibiting nonconsensual porn.[194] At a minimum, it is often possible for social media companies to determine the physical location of an anonymous user with some precision using geolocation data.[195] This data can be used to narrow down the area in which potential posters live and/or work, making it easier to identify possible perpetrators and defendants.

Given the protections afforded to anonymous posters on the internet, First Amendment protections for many kinds of speech, the widespread social expectation and tradition that people may speak anonymously online, and the technological difficulties inherent in identifying the real identities of unknown speakers, it is unlikely that nonconsensual porn victims will be able to unmask anonymous posters through private action that does not involve cooperation by an ISP or ICP. For that reason, it is necessary to reexamine the role that ICPs in particular play in the growth and spread of nonconsensual porn and the extent to which ICPs should be incentivized to stem this growth.

IV. THE COMMUNICATIONS DECENCY ACT SHOULD INCENTIVIZE ICP DETERRENCE

While improving the ability to identify perpetrators is a critical step, ICPs can also do more to deter and stem the growth of nonconsensual porn in other ways. Many social media companies have begun to do this voluntarily, which should be lauded. As is true with any voluntary effort, however, these practices can be withdrawn at any time. A comprehensive review of what ICPs can do to fight the nonconsensual porn epidemic, whose growth they have unintentionally

---

191. *What Names Are Allowed on Facebook?* FACEBOOK, https://www.facebook.com/help/112146705538576 (last visited Jan. 19, 2018).

192. Rebecca MacKinnon & Hae-in Lim, *Google Plus Finally Gives Up on Its Ineffective, Dangerous Real-Name Policy*, SLATE: FUTURE TENSE (July 17, 2014 3:19 PM) http://www.slate.com/blogs/future_tense/2014/07/17/google_plus_finally_ditches_its_ineffective_dangerous_real_name_policy.html.

193. *Nymwar*, TECHOPEDIA, https://www.techopedia.com/definition/29486/nymwar (last visited Jan. 19, 2018).

194. *See* notes 207-208 *infra* and accompanying text.

195. Vijay, *Social Media Apps Can Disclose Anonymous Users Through Location Data*, TECHWORM (Apr. 17, 2016), https://www.techworm.net/2016/04/social-media-apps-can-disclose-identity-users-location-data.html

facilitated, should include a review of their role in stopping nonconsensual porn posts before or shortly after they occur. As a first matter, however, it is necessary to reexamine the protections of the CDA.

A. The CDA Shields ICPs from Liability for Nonconsensual Porn

Nonconsensual porn victims generally cannot sue ICPs for damage done by anonymous posters because of the CDA's safe harbor provision.[196] As a general matter, the CDA shields social media companies and other ICPs from direct liability based on the information others publish on their networks. Section 230 of the CDA states that "no provider… of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[197] The CDA notes that "[i]ncreasingly Americans are relying on interactive media for a variety of political, educational, cultural and entertainment services."[198] It also underscores the United States' policy to "promote the continued development of the Internet … and other interactive media."[199]

In one of the first cases to interpret the CDA, the Fourth Circuit Court of Appeals observed that Section 230 "plainly immunizes computer service providers like AOL from liability for information that originates with third parties."[200] The plaintiff in that case had been targeted by an anonymous online poster who had advertised items glorifying the bombing of the Alfred P. Murrah Federal Building in Oklahoma six days after the bombing took place and listed the plaintiff's telephone number as contact information.[201] The plaintiff sued AOL for negligence in failing to prevent the re-posting of these allegedly defamatory advertisements after their removal. The court held that the CDA shielded AOL from liability under common law negligence claims.

In explaining its rationale, the court observed that Congress enacted the CDA in order to protect online service providers from tort liability based on what its customers post.[202] Given the massive numbers of online users, it reasoned that Congress had decided that service providers would have to restrict communication too much if they were liable for its content:

> The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and

196. *See, e.g.*, Caraccioli v. Facebook, No. 5:15-cv-04145-EJD (9th Cir. June 6, 2017), available at http://cdn.ca9.uscourts.gov/datastore/memoranda/2017/06/06/16-15610.pdf, at 2-3 (holding that Facebook is not liable for nonconsensual porn posted on it because it is an "information content provider" within the meaning of the CDA).

197. 47 U.S.C. §230 (c)(1) (1996).

198. Communications Decency Act of 1996, 47 U.S.C. §230 (c)(1) (1996).

199. 47 U.S.C. §230 (b)(1) (1996).

200. Zeran v. America Online, Inc., 129 F.3d 327, 328 (4th Cir. 1997), *cert. denied*, 524 US 937 (1998).

201. *Zeran*, 129 F.3d 327 at 329.

202. *Zeran*, 129 F.3d 327 at 328.

chose to immunize service providers to avoid any such restrictive effect.[203]

But the CDA does not immunize online service providers from all liability. It does not restrict the federal government's ability to deter criminal activity and enforce criminal law.[204] Indeed, the Act itself notes that "it is the policy of the United States … to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer."[205] In other words, the CDA's provisions will not bar a provider of online services from liability in connection with certain crimes facilitated by internet use.

One concern an ICP may have about removing harassing posts is the threat of liability from the posters themselves. The CDA protects them against precisely this type of claim, even when the poster claims that they have a right to be heard under the First Amendment. The CDA explicitly protects any "provider or user of an interactive computer service" from liability based on any voluntary restriction or removal of material that the provider or user finds to be "obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable, whether or not such material is constitutionally protected."[206]

B. ICPs' Efforts to Combat Nonconsensual Porn Are Helpful and Insufficient

Some social media companies take it upon themselves to address the potential harm caused by anonymous sources by providing ways to report hate speech or harassment. Microsoft, Google, Facebook, Twitter, and Reddit developed policies prohibiting nonconsensual porn in 2015.[207] Twitter's revised rules, for example, "prohibit the posting or sharing of intimate photos or videos that were or appear to have been taken or distributed without the subject's consent."[208] As a consequence of posting such material, Twitter "will suspend any account [it identifies] as the original poster of intimate media that has been produced or distributed without the subject's consent," and will also suspend accounts dedicated to nonconsensual porn.[209] Instagram and Tumblr also developed removal policies for nonconsensual porn.[210]

Such self-regulation is helpful, yet limited in its scope and effectiveness. For example, many reporting mechanisms process complaints according to an algorithm rather than subjecting reports to human review, and do not allow people reporting abuse to challenge automated responses that are inaccurate or inadequate. Self-regulation is also voluntary, and can be withdrawn or scaled back

203. *Zeran*, 129 F.3d 327 at 331.

204. 47 U.S.C. §230 (e)(1) (1996).

205. 47 U.S.C. §230 (b)(5) (1996).

206. 47 U.S.C. §230 (c)(1) (1996).

207. Carrie Goldberg, *How to Report Revenge on Social Media*, C.A. GOLDBERG (Jul. 25, 2015) https://carrie-goldberg.squarespace.com/report-revenge-porn-on-social-media.

208. *About Intimate Media on Twitter*, TWITTER, https://help.twitter.com/en/rules-andpolicies/intimate-media (last visited January 17, 2018).

209. *Id.*

210. Casey Johnston, *How to Report Social Media Harassment: A Practical Guide*, LENNY (Jul. 19, 2016) http://www.lennyletter.com/culture/a474/how-to-report-social-media-harassment-a-practical-guide/.

when these companies decide that it is no longer in their interest to provide a reporting service. There is little external incentive for social media companies to provide consistent, reliable unmasking responses. Indeed, many may fear that the accused users would sue for violation of what they consider to be their rights of anonymity.

Perhaps the most promising means of unmasking anonymous harassers is the voluntary and collaborative efforts of the ICPs who host them. Although there has been great resistance to social media companies' real name policies as a general matter, including the nymwars, there is reason to believe that there may be less resistance to unmasking in the context of online harassment. Much of the resistance to real-name policies stemmed from the fact that drag queens and other marginalized members of society relied on fake names for a variety of beneficial, or at least innocuous reasons, and saw the real-name policies as a means of marginalizing them further.[211] There is no comparable social benefit in shielding alleged nonconsensual porn posters from criminal prosecution or civil liability.

Social media companies have cooperated in unmasking a different kind of assailant: terrorists. Spurred in part by criticism that they have not done enough to monitor and deter terrorism, Facebook, Twitter and Google have been devoting increased resources to finding and removing terrorist propaganda videos and to shutting down accounts linked to violent terrorist groups.[212] Advertiser boycotts and lawsuits are compelling them to do so.[213] While these companies have relied largely on user reports to flag potential offenders, new techniques are being developed, including algorithms that identify signature images of terrorist content.[214] This technique is similar to PhotoDNA, which matches images posted online with those in the National Center for Missing & Exploited Children's image database.[215] There is some debate, however, over the effectiveness of these new techniques and the probability of their long-term success, especially with regard to their ability to screen video content.[216] Nonetheless, in a joint statement in December 2016, Facebook, Microsoft, Twitter and YouTube pledged to create a shared database of unique digital signifiers for violent terrorist imagery, in an effort to "curb the pressing global issue of terrorist content online."[217]

Facebook is also taking some degree of responsibility for monitoring other kinds of domestic violence. Police and prosecutors in the Chicago area attribute a rise in the number of gang-related murders there in part to social media and streaming platforms such as Facebook Live, which launched in 2016.[218] They

---

211. *See* MacKinnon and Lim, *supra* note 192.

212. Larry Greenmeier, *When Hatred Goes Viral: Inside Social Media's Efforts to Combat Terrorism*, SCIENTIFIC AMERICAN (May 24, 2017) https://www.scientificamerican.com/article/when-hatred-goes-viral-inside-social-medias-efforts-to-combat-terrorism/.

213. *Id.*

214. *Id.*

215. *Id.*

216. *Id.*

217. *Partnering to Help Curb Spread of Online Terrorist Content*, FACEBOOK: NEWSROOM (Dec. 5, 2016) https://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/.

218. Shibani Mahtani, *Social Media Emerges as New Frontier in Fight Against Violent Crime*, WALL ST. J. (Nov. 24, 2017) https://www.wsj.com/articles/social-media-emerges-as-new-frontier-in-

believe that social media exacerbates a culture of violence and helps escalate disputes. A state's attorney for Cook County said that these platforms "pour[] an accelerant on what was already there." Facebook responded to journalists' inquiries about this connection by noting that it would double the number of employees reviewing content on Facebook for dangerous and hateful speech to 20,000 in 2018, up from 10,000 in 2017.

The same can and should be done with regard to the most tortious forms of online harassment. If social media companies can develop new tools and devote more resources to detecting and deterring terrorism, they can take similar steps toward combating online harassment. They can, for example, join forces to develop a shared database of revenge porn imagery and language commonly used by the online mobs who cause the amplification effects that terrorize so many victims. They can collaborate to develop more efficient ways of deterring nonconsensual porn, and they can make a public statement of their intent to do so. Taking a public and concerted stand against this kind of online harassment would be more than just symbolic. It would establish a stronger industry intolerance for tortious hate speech, cyberstalking and harassment that would affect putative harassers and, in all likelihood, reduce the number of victims and the extent of their harassment.

Facebook, in fact, is already running programs to streamline the removal of nonconsensual porn in other countries. In November 2017, Facebook announced an experimental strategy in Australia to "help prevent non-consensual intimate images from being posted and shared anywhere on Facebook, Messenger and Instagram."[219] In this pilot program, users are asked to send Facebook the images they are concerned about via Messenger. Facebook then "hashes" those images, giving them a unique digital fingerprint that can be used to stop further distribution of those images. In this program, Facebook is partnering with an Australian government agency that focuses on electronic safety. A study released in May 2017 reported that 23 percent, or one in five, Australians between the age of 16 and 49 reported being subject to "image-based abuse."[220] This was defined to include images showing breasts or genitals, including pictures taken during showering or bathing and "upskirting and downblousing."[221]

Supporters lauded the program because it allows both victims of nonconsensual porn and people who are worried about becoming nonconsensual porn victims to take preventative action.[222] Critics expressed concern, among other things, that Facebook's solution required victims and potential victims of nonconsensual porn to post their images proactively, trusting that Facebook staff

---

fight-against-violent-crime-1511528400.

219. *The Facts: Non-Consensual Intimate Image Pilot*, FACEBOOK: NEWSROOM (Nov. 9, 2017) https://newsroom.fb.com/news/h/non-consensual-intimate-image-pilot-the-facts/.

220. Nicola Henry et al., NOT JUST 'REVENGE PORNOGRAPHY': AUSTRALIANS' EXPERIENCES OF IMAGE-BASED ABUSE: A SUMMARY REPORT (2017) https://www.rmit.edu.au/content/dam/rmit/documents/college-of-design-and-social-context/schools/global-urban-and-social-studies/revenge_porn_report_2017.pdf.

221. *Id.*

222. Olivia Solon, *Facebook Asks Users for Nude Photos in Project to Combat Revenge Porn*, THE GUARDIAN (Nov. 7, 2017) https://www.theguardian.com/technology/2017/nov/07/facebook-revenge-porn-nude-photos.

would handle them appropriately, when Facebook has shown itself repeatedly to be something less than trustworthy.[223] One observer suggested that a better approach would not involve disclosure of the image at all, but rather a telephone call to Facebook alerting them to the problem.[224] Any approach that does not specify a particular problematic image, however, is unlikely to succeed. Whether the monitoring, prohibition and/or removal of nonconsensual porn is done by a government agency, a social media company such as Facebook, or a combination thereof, it will be critical to know which images are nonconsensual and which are consensual so that the removal of images does not intrude into the realm of voluntary self-expression.

Another solution ICPs should consider is the development of an internal flagging system that warns likely harassers that they may be about to break the law before they post. One scholar has proposed that web hosts might warn users who are about to post shaming language of the consequences of doing so by using algorithms and filters designed to detect that activity.[225] Warning potential nonconsensual porn posters of the potential consequences of their actions would make it easier to argue that those who post nonconsensual porn regardless of the warnings have the mens rea of recklessness, which the Model Penal Code defines as "consciously disregard[ing] a substantial and unjustifiable risk that the material element exists or will result from this conduct."[226]

C. ICPs Should Be Compelled to Deter Nonconsensual Porn

Facebook's voluntary efforts to deter nonconsensual porn work as long as Facebook chooses to engage in them. For these methods to be enduringly effective, however, they must be compulsory. In order to make such measures compulsory, it may be necessary to amend the CDA to remove the shield it currently provides for ICPs. One of the assumptions underlying the passage of the CDA was that it would be too cumbersome for online service providers to monitor their users' posts for potentially harmful content.[227] Given the subsequent developments in search technology, that is no longer necessarily true.

More than twenty years after the enactment of the CDA, it is time to reexamine the wisdom of that law's broad shield. As other scholars have observed, the CDA no longer makes sense as a matter of technology policy. Some have suggested that Congress amend the CDA to include notice and takedown provisions for online harassment, similar to those of the Digital Millennium Copyright Act.[228] Such provisions could require social media companies and ISPs

223. Van Badham, *Sending In Our Nude Photos to Fight Revenge Porn? No Thanks, Facebook*, THE GUARDIAN: OPINION (Nov. 12, 2017) https://www.theguardian.com/commentisfree/2017/nov/13/sending-in-our-nude-photos-to-fight-revenge-porn-no-thanks-facebook.

224. *Id.* (stating "[y]ou shouldn't need to send naked pictures of yourself to register an abuse. All you should have to do is make a phone call and action should be taken on your behalf").

225. Kristine L. Gallardo, *Taming the Internet Pitchfork Mob: Online Public Shaming, the Viral Media Age, and the Communications Decency Act*, 19 VAND. J. ENT. & TECH. L. 721, 732 (2017).

226. MODEL PENAL CODE §2.02 (Am. Law Inst. 1981).

227. *Zeran*, 129 F.3d at 330-31.

228. See Olivera Medenica & Kaiser Wahab, *Does Liability Enhance Credibility? Lessons from the DMCA Applied to Online Defamation*, 25 CARDOZO ARTS & ENT. L.J. 237, 239 (2007) (advocating for

to remove online harassment when it is flagged as such. Under both proposals, social media companies and ISPs would take a far more active role in detecting and deterring online harassment. While the CDA presumes that ICPs and social media companies should take a passive role with regard to online content, these more recent proposals, together with the sharp rise in frequency and corrosiveness of online harassment, envision a more active and socially responsible role for web hosts.

The United States may not be the first country to hold ICPs legally responsible for doing too little to stop the spread of nonconsensual porn. Recent proceedings in Northern Ireland suggest that Facebook may come under greater legal pressure to deter nonconsensual porn elsewhere in the world. In January 2018, the High Court in Belfast confirmed the settlement of a case in which a 14 year old victim of nonconsensual porn sued Facebook for failing to block the re-publication of her photo after she notified the company that it was taken without her consent.[229] Because there was no judgment against Facebook, the case has no precedential value, but it suggests that there is a greater risk of potential liability for an ICP's failure to stop nonconsensual porn images from spreading than many industry analysts may have expected.[230] In the wake of the settlement, lawyers reported being "deluged" with queries from nonconsensual porn victims interested in suing Facebook.[231]

In the United States, some courts are already starting to question whether the CDA should provide a complete shield for ICPs in similar cases. In at least one case, a court has held a social media company liable for failure to warn some users about likely harm from other users. It concerned a model who alleged that a website was negligent under California law for failing to warn her about two website users' practice of using the site to drug and rape models like her.[232] In that case, plaintiff Jane Doe subscribed to the website Model Mayhem, a networking site for models, operated by defendant Internet Brands.[233] Two men used the site to identify women, whom they contacted posing as agents, and lure them to a fake modeling audition in Florida.[234] The men then drugged their victims, raped them, and videotaped their acts for distribution as pornography.[235] Doe became one of these victims.[236] She alleged that Internet Brands knew about the rape scheme but

---

DMCA-styled notice and takedown provisions to be added to Section 230 of the CDA).

229. Alan Erwin, *Girl (14) Settles Landmark Action Against Facebook Over Naked Images*, IRISH TIMES (Jan. 9, 2018), https://www.irishtimes.com/news/crime-and-law/courts/high-court/girl-14-settles-landmark-action-against-facebook-over-naked-images-1.3349974.

230. See Jamie Rigg, *Facebook Settles Out of Court in Unique Revenge Porn Case*, ENGADGET (Jan. 16, 2018), https://www.engadget.com/2018/01/16/facebook-revenge-porn-settlement/ ("For anyone considering a similar civil suit against Facebook, Twitter or others, there's now an example of someone *sorta* winning. Not a precedent, but something close.")

231. Henry McDonald, *Facebook Warned It Faces Legal Action From 'Revenge Porn' Victims*, GUARDIAN (Jan. 12, 2018), https://www.theguardian.com/technology/2018/jan/12/facebook-faces-legal-action-from-victims-of-revenge-porn.

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

233. *Id.*

234. *Id.*

235. *Id.*

236. *Id.*

failed to warn website users of the risks.[237] Internet Brands had moved to dismiss her claims as barred by the CDA, and the district court granted its motion.[238] The Court of Appeals for the Ninth Circuit reversed.[239]

In holding for Doe, the court concluded that the CDA did not shield Internet Brands from negligence liability because Doe did not seek to hold it liable as the "publisher or speaker" of any particular content.[240] Instead, Doe alleged that the Internet Brands had a duty to warn users of the dangers of the rape scheme, a duty it could have fulfilled by posting a notice on the Model Mayhem website.[241] The court reasoned that an "alleged tort based on a duty that would require such a self-produced warning falls outside of" the protections of the CDA.[242] In so holding, the court noted that its conclusion was consistent with one of the CDA's core policies, "to provide '[p]rotection for 'Good Samaritan' blocking and screening of offensive material.'" Given that purpose, it stated, "a website should be able to act as a 'Good Samaritan' to self-regulate offensive third party content without fear of liability."[243] In light of the court's ruling on Doe's negligence claim, the court did more than allow a website to act as a Good Samaritan; it also suggested the possibility that the website has a duty to warn once a provider knows or should have known of a likely danger to users.

There are many ways for a website to know of such potential dangers. Most social media companies have established a method by which people can alert the company to potentially dangerous or inappropriate content.[244] Future plaintiffs using this case as precedent might argue that once a website is on notice of likely potential harm, its duty to warn under state negligence laws may be triggered.

After concluding that the CDA did not bar Doe's claims, the court in Internet Brands dismissed the claim that its holding might have an impermissible chilling effect on online speech. It noted that the CDA does not provide a general shield against liability for online service providers. "Congress has not provided an all-purpose get-out-of-jail-free card for businesses that publish user content on the internet, though any claims might have a marginal chilling effect on internet publishing businesses." By articulating some of the CDA's limitations, this case illuminates the possibility that users might hold websites more accountable for the harms they knowingly, or negligently, facilitate.

Social media companies may be compelled to remove images when their rightful owners can establish that their copyright has been violated. As one observer noted, however, "using copyright law to combat revenge porn is a bit

237. *Internet Brands, Inc.*, 824 F.3d at 848.

238. *Internet Brands, Inc.*, 824 F.3d at 846.

239. *Internet Brands, Inc.*, 824 F.3d at 853.

240. *Internet Brands, Inc.*, 824 F.3d at 851.

241. *Id.*

242. *Id.*

243. *Internet Brands, Inc.*, 824 F.3d at 850.

244. *See, e.g.*, *Reporting Abuse*, FACEBOOK, https://www.facebook.com/help/1753719584844061?helpref=hc_global_nav (last visited Jan. 6, 2018) (noting that "[w]hen something gets reported to Facebook, we review it and remove anything that goes against the Facebook Community Standards" and providing reporting link).

like using tax law to go after Al Capone."[245] Another option would be the establishment of maximum response times to user allegations of tortious content. As noted above, most social media companies have established a method by which people can alert the company to potentially dangerous or inappropriate content.[246] Whether and when the companies respond to such alerts, however, is up to them. Social media companies might voluntarily institute time limits by which they ensure a detailed written response to user alerts, possibly including a statement as to what, if any, actions were taken as a consequence of the alert. Alternatively, states or the Federal Communications Commission might compel social media companies to institute both the alert service and a maximum response time.

In light of the many benefits of online anonymity, it would be unwise as a matter of policy and likely impossible as a matter of law to do away with it entirely. That said, the increasing danger of online harassment, stalking, and other potentially serious harms underscore the need to revisit the issue of whether social media companies and ISPs should be legally required to make it easier for abusive posters to be unmasked.

D. Reforms Should Ensure That Perpetrators Account For Their Actions

ICPs should not have sole responsibility for curbing nonconsensual porn simply because they can police it more effectively than the legal system alone. One danger of shifting too much responsibility to ICPs for nonconsensual porn, or any other social ill, is that it risks attributing too little responsibility to the individual perpetrators themselves. Ultimately, it should be the people who post nonconsensual porn who are the focus of educational, social and regulatory reforms. No comprehensive program to stem the spread of nonconsensual porn should in effect absolve the people who choose to post nonconsensual private images of other people on the internet, as it is those individual decisions to post that create the harm in the first place.

Clearer legal definitions of nonconsensual porn and its consequences are necessary to effect a better balance between the rights of nonconsensual porn victims and accused perpetrators without unduly burdening ICPs. A significant part of the solution, however, lies beyond what legal reforms can accomplish, and may include broader educational efforts to emphasize the wrongs and harms of nonconsensual porn as well as public service announcements and other non-legal strategies. In light of the prevalence of nonconsensual porn, the legal and cultural permissiveness about anonymity online in the U.S., and the limitations that such permissiveness places on even well intentioned regulatory reform, focusing on the individual posters alone is unlikely to be effective at least in the short term. Recalibrating our standards of anonymity for nonconsensual porn victims in both civil and criminal cases, and reassessing the extent to which ICPs should be liable for nonconsensual porn that they know or should know they are hosting and promulgating, is the best next step towards eliminating nonconsensual porn.

245. Talbot, *supra* note 111, at 56.

246. *Reporting Abuse*, *supra* note 240.

V. CONCLUSION

The sharp rise and high cost of nonconsensual porn impose a significant burden on members of society who are already on the political margins. They demand a qualitative change in our legislative and technological responses to this form of online speech. The lack of coherent state regulation of nonconsensual porn, despite its recent growth, underscores the need for greater protection of the identities of nonconsensual porn victims. So too does the lack of anonymity provisions in the IPPA and earlier efforts to regulate nonconsensual porn at the federal level. At the same time, legal protections of internet service providers and social media companies do too much to shield online perpetrators and too little to allow victims of anonymous harassment to justice.

Traditional assumptions about and arguments in favor of victim identification and online anonymity may, in the context of nonconsensual porn, be superseded by the necessity of technological and employment practice developments that flip those values. A comprehensive improvement in access to justice for nonconsensual porn victims would permit both more pseudonymity for victims and less anonymity for alleged offenders. It should be more difficult for anonymous online harassers to remain anonymous and it should be easier for their victims to sue as anonymous plaintiffs. In addition, ICPs should be compelled to do more to uncover and deter anonymous online harassment using the same tools and collaborative techniques they already use to fight terrorism. As the spread and damages of nonconsensual porn have changed, the public and private response to such harassment should change as well in order to provide greater protection to the most marginalized victims. If there is a right to anonymous speech online, that right should be superseded by the right to safely bring an alleged nonconsensual porn poster to justice.

While ICPs have begun to change their practices regarding nonconsensual porn posting, more must be done. It is only when the structures that facilitate the rise of nonconsensual porn are required to stem that spread, and when its victims are confident in the protections afforded by the legal system, that the intent behind the rising regulation of nonconsensual porn truly can be put into effect.