Let Me Tell You Who I Am: Establishing a Federal Remedy for Interference with Online Identity

Laura K. Hamilton*

TABLE OF CONTENTS

* J.D., The George Washington University Law School, May 2017. Senior Publications Editor, *Federal Communications Law Journal*, 2016–17. B.A., History with Honors, Minors in Middle Eastern Studies & French, New York University, 2011. This Note is dedicated to the late Jill N. Claster of New York University, to whose grace, wit, and intelligence I will always aspire. The author would also like to thank Professors Peter J. Smith and Orin Kerr of The George Washington University Law School for shepherding this Note's thesis along (knowingly or not). Special thanks goes to Mona Sedky and the prosecutors of the Computer Crime & Intellectual Property Section of the Department of Justice. The author would also like to recognize Dr. Holly Jacobs for her continuing work on behalf of victims.

I. FOREWORD

Since this Note's conception in the fall of 2015, the politics of online speech have changed dramatically. As of January 2017, the specter of a weakened First Amendment continues to spur debate—with the press, in particular, being admonished.[1] At the same time, women's rights and sexual freedoms have also become increasingly controversial.[2] Striking the proper balance between protecting individual rights and buttressing the First Amendment has never been more important. Accordingly, this Note argues that this delicate balance can, and should, be struck by careful and comprehensive federal legislation.

II. INTRODUCTION

The Internet disrupts. From Fort Meade to Silicon Valley, concerns about online identity resonate. Can members of "Anonymous" remain truly anonymous?[3] What happens when Twitter can't verify a person's identity?[4] Will there come a time when we can no longer separate fact from fiction on the Internet?

A distinct personal identity and the right to reinvention are quintessential American ideals. In 2015, the New York Times published an article branding that year "The Year We Obsessed Over Identity."[5] As the Internet becomes increasingly intertwined with all aspects of human life—such as medical care, shopping lists, mobile payments, travel documents—it is becoming increasingly difficult to separate a person's online identity from who the person is in the physical world. For most Internet users, it is unlikely

---

1. *See, e.g.*, Stephen Collinson, *Trump takes aim at First Amendment*, CNN (Nov. 30, 2016, 7:34 AM EDT), http://www.cnn.com/2016/11/29/politics/donald-trump-first-amendment [https://perma.cc/TQA4-36L4]; Michael M. Grynbaum, *Trump Strategist Stephen Bannon Says Media Should 'Keep Its Mouth Shut'*, N.Y. TIMES (Jan. 26, 2017), https://www.nytimes.com/2017/01/26/business/media/stephen-bannon-trump-news-media.html [https://perma.cc/WSQ5-4Q9R].

2. *See, e.g.*, Yamiche Alcindof & Susan Chira, *Defiant Voices Flood U.S. Cities as Women Rally for Rights*, N.Y. TIMES (Jan. 21, 2017), https://www.nytimes.com/2017/01/21/us/women-march-protest-president-trump.html [https://perma.cc/RC6Q-YPLA]; Jeremy W. Peters, *Trump on Their Side, Conservatives See Hope in Lengthy Abortion Fight*, N.Y. TIMES (Jan. 26, 2017), https://www.nytimes.com/2017/01/26/us/politics/democrats-republicans-planned-parenthood.html [https://perma.cc/MGN5-DH6A].

3. *See*, *e.g.*, Betsy Isaacson, *7 Anonymous Hackers Who Have Been Unmasked*, HUFFINGTON POST (Jun. 7, 2013), http://www.huffingtonpost.com/2013/06/07/anonymous-hackers_n_3398282.html [https://perma.cc/R6QC-3U3W].

4. *See, e.g.*, Rebecca Greenfield, *The Ethics of Fake Twitter Accounts*, WIRE (Feb. 1, 2012), http://www.thewire.com/technology/2012/02/learning-cormac-mccarthy-twitter-hoax/48147 [https://perma.cc/FAZ9-BDNG].

5. Wesley Morris, *The Year We Obsessed Over Identity*, N.Y. TIMES MAGAZINE (Oct. 6, 2015), http://www.nytimes.com/2015/10/11/magazine/the-year-we-obsessed-over-identity.html [https://perma.cc/T3BH-UY6Z].

that these two identities will differ significantly.[6] When individuals suffer from non-consensual pornography ("NCP"), popularly known as "revenge porn," separating offline fact from online fiction is difficult, expensive, and often impossible.[7] This Note will focus on the novel harms arising out of our dependency on the Internet, examine the current legislative landscape in the United States, and recommend that a federal statute should provide a remedy for individuals whose online identities are maliciously compromised.

There are two general categories of harm that flow from tampering with online identity: (1) reputational harm, and (2) "historical" harm. Reputational harm concerns "true" statements that,[8] due to the Internet's unparalleled ability to reach a global audience, are expanded beyond their original scope such that the individual's reputation in the broader community is denigrated disproportionately. The consequences of reputational harm on an individual can be economic (e.g., job loss[9]), as well as emotional and physical (e.g., loss of friendships, depression,[10] and even suicide[11]).

"Historical" harm, by contrast, concerns "false" online facts substituted for the offline truth, such that consumers of this information are unable to parse historical reality from fantasy. In extreme cases, individuals relying on

---

6. Tomas Chamorro-Premuzic, *How Different are Your Online and Offline Personalities?*, GUARDIAN (Sept. 24, 2015), https://www.theguardian.com/media-network/2015/sep/24/online-offline-personality-digital-identity [https://perma.cc/UP2D-ZD4S] ("[O]nline activities are no longer separable from our real lives, but an integral part of it.").

7. Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 346 (2014). This is fundamentally distinct from the idea of "poster's remorse," where an Internet user comes to regret something they have voluntarily uploaded. Lance Whitney, *Poster's remorse common for social-network users*, CNET (May 18, 2010, 11:03 AM), http://www.cnet.com/news/posters-remorse-common-for-social-network-users [https://perma.cc/EA33-E8U7]. Though some scholars have made compelling arguments to counteract the Internet's perfect memory by integrating an expiration date for information, for example, and the European Union has instituted the "Right to be Forgotten"— that discussion is regrettably outside the scope of this Note. *See, e.g.*, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN [https://perma.cc/V4ZE-27HW]; VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 15 (4th prtg. 2011); *see also Factsheet on the "Right to be Forgotten" Ruling (C-131/12)*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf [https://perma.cc/2N97-P547] (last visited Apr. 6, 2016).

8. There is much ongoing controversy, especially in a First Amendment context, on the question of how much the law can dictate what is "true" online. Given the potentially endless breadth of this topic, what online speech should qualify as "true" is not discussed. *See generally* Yasmine Agelidis, Note, *Protecting the Good, the Bad, and the Ugly: "Exposure" Data Breaches and Suggestions for Coping with Them*, 31 BERKELEY TECH. L.J. 1057, 1057 (2016).

9. *See* Jon Ronson, *How One Stupid Tweet Blew Up Justine Sacco's Life*, N.Y. TIMES MAGAZINE (Feb. 12, 2015), http://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html [https://perma.cc/92ZF-79EH].

10. *See id.*

11. Michelle Dean, *The Story of Amanda Todd*, NEW YORKER MAGAZINE (Oct. 18, 2012), http://www.newyorker.com/culture/culture-desk/the-story-of-amanda-todd [https://perma.cc/F4MP-P643].

false online information have committed violent crimes.[12] There is often an overlap between the two categories: NCP could be considered reputational harm, for the original photographs are generally consensual, and it may also be considered historical harm, as the original photos can be altered in Photoshop or posted alongside false statements. Clearly delineating the types of harm the federal statute is designed to prevent is crucial to understanding the feasibility of introducing legislation.

The most obvious and important obstacle to such legislation is the First Amendment. It is also important to recognize and appreciate that the First Amendment plays a crucial role in cabining laws that seek to control activity and speech on the Internet.[13] But the First Amendment does not fully protect defamation or libel, and the Supreme Court has ruled that a private figure need not demonstrate malice in a defamation suit in order to recover.[14]

In the United States, we are increasingly concerned with historical harm arising out of NCP, identity theft, and data privacy.[15] Section III of this Note will examine the landscape of existing legislation and explain the development of applicable tort law, ultimately concluding that neither is sufficient to address modern harms. Section IV will propose a recommendation for enacting comprehensive federal legislation. Recognizing the Internet's broad scope, the need for uniformity across state lines, and the current lack of redressability for actual harm, the proposed federal statute will allow for both civil and criminal causes of action to protect individuals from malicious interference with their online identity.

III. BACKGROUND

"Right or wrong, the [I]nternet is a cruel historian."[16] The twenty-first century has been characterized by a perfect storm of identity information technology. With the emergence of Facebook, a billion users logged on "in a single day" in 2015 to interact on a website not dissimilar to an online Rolodex.[17] Sergey Brin and Larry Page developed a smart search engine in Google that aims to provide users with more accurate and more detailed

12. *See* DeeDee Correll, *Former boyfriend used Craigslist to arrange woman's rape, police say*, L.A. TIMES (Jan. 11, 2010), http://articles.latimes.com/2010/jan/11/nation/la-na-rape-craigslist11-2010jan11 [https://perma.cc/FWD3-4EHY].

13. While the Supreme Court has not directly addressed this proposition, it is widely presumed and for purposes of this Note not especially controversial. *See* Reno v. ACLU, 521 U.S. 844, 870 (1997) ("[O]ur cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to [the Internet].").

14. *See* David S. Ardia, *Reputation in a Networked World: Revisiting the Social Foundations of Defamation Law*, 45 HARV. C.R.-C.L. L. REV. 261, 281 (2010) (citing Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749 (1985)).

15. *See, e.g.*, Citron & Franks, *supra* note 7; *see also* Alina Tugend, *Oh, No! My Identity's Gone! Call the Insurer.*, N.Y. TIMES:BUSINESS DAY (May 28, 2005), http://www.nytimes.com/2005/05/28/business/oh-no-my-identitys-gone-call-the-insurer.html?_r=0 [https://perma.cc/AW56-Z8VF].

16. DANIEL J. SOLOVE, THE FUTURE OF REPUTATION, GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 11 (2007).

17. Mark Zuckerberg, FACEBOOK (Aug. 27, 2015, 4:33pm), https://www.facebook.com/zuck/posts/10102329188394581 [https://perma.cc/53L3-62ZC].

information than ever before.[18] The inevitable result is that more information about a person's online identity is readily available, with an extraordinarily low barrier to entry. And, in a post-Snowden world, many Americans no longer expect privacy in online communications[19], whatever the federal courts may hold.[20] Once information is disseminated online, it is impossible to take back.[21] As a fictionalized Erica Albright, Mark Zuckerberg's ex-girlfriend, declares in *The Social Network*, "the Internet's not written in pencil, Mark, it's written in ink."[22] The Internet is permanent.[23]

A. Modern Problems Mandate Modern Solutions

NCP is a quintessential example of malicious interference with online identity that encompasses both reputational and historical harm. In November 2011, Holly Jacobs received an anonymous email stating, "someone is trying to make life very difficult for you."[24] The email contained a link to a site that

---

18. *What We Do*, GOOGLE, https://www.google.com/about/company/products [https://perma.cc/XTN6-LMJK] (last visited Feb. 27, 2016).

19. *See, e.g.*, Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RES. CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ [https://perma.cc/D5GK-5C2Z] (finding 91% of those surveyed "agree" or "strongly agree" that consumers have lost control over how personal information is collected or used by companies); Timothy J. Geverd, *Bulk Telephony Metadata Collection and the Fourth Amendment: The Case for Revisiting the Third-Party Disclosure Doctrine in the Digital Age*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 191, 193 ("[I]n the wake of the Edward Snowden leaks, federal courts will be forced to consider the continued vitality of the third-party disclosure doctrine in today's technological age."); John Levin, *The Cloud and the NSA*, C2014BA Rec., April/May , at 38 ("I believe that Snowden's disclosures make it safe to say that nothing that is transmitted through or stored in the cloud is confidential.").

20. *Compare* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (holding that a reasonable expectation of privacy exists in the contents of email communications), *with* Rehberg v. Paulk, 598 F.3d 1268, 1281 (11th Cir. 2010) ("A person also loses a reasonable expectation of privacy in emails, at least after the email is sent to and received by a third party."), *vacated on panel reh'g on other grounds*, 611 F.3d 828 (11th Cir. 2010).

21. *See, e.g.*, Ronson, *supra* note 9; Katie Mettler, *What Rob Kardashian did to Blac Chyna could be 'revenge porn,' lawyers say, and illegal*, WASH. POST (July 6, 2017), https://www.washingtonpost.com/news/morning-mix/wp/2017/07/06/what-rob-kardashian-did-to-blac-chyna-could-be-revenge-porn-lawyers-say-and-illegal/ [https://perma.cc/FWL4-MHC4] ("Even though Instagram quickly shut down his account, Kardashian managed to move the rant and nude photos temporarily to Twitter, before that social platform also blocked the revealing photo. But just within the few minutes the nude picture was online, it got thousands of retweets and was likely screenshot just as many times . . . .").

22. THE SOCIAL NETWORK (Columbia Pictures 2010). Though Erica Albright is a real person, the quote is fictional. It does, however, perfectly encapsulate a common theme in modern Internet use. Other commentators have been less artful. As Chief Judge Kozinski of the Ninth Circuit described it: "They say that removing something from the internet is about as easy as removing urine from a swimming pool, and that's pretty much the story." Alex Kozinski, Symposium Keynote, *The Dead Past*, 64 STAN. L. REV. ONLINE 117, 124 (Apr. 2012).

23. *See* MAYER-SCHÖNBERGER, *supra* note 7, at 68–69 ("[I]t is obvious that not just individuals, but private as well as public organizations, too, experience the consequences of permanent comprehensive memory.").

24. *See* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 45 (2014).

hosted nude photos of her and an explicit video taken during a former relationship.[25] Googling her name revealed the images appeared on hundreds of other sites as well.[26] Perhaps the most horrifying detail, however, was that the posts were not limited to revealing photos, but also included contact information about her offline identity, such as her full name, email address and Facebook page.[27] When Jacobs initially approached the Miami police and the FBI, both disclaimed the existence of any legal remedies, despite several federal laws criminalizing cyberstalking and online harassment.[28] At a loss, she even resorted to copyright law by sending the linking websites takedown notices, arguing she was the original creator and owner of the nude photographs.[29]

In exposing sensitive photographs to the Internet, NCP causes reputational harm in publishing "true" facts (real photographs of a victim's naked body) to a broader audience than intended, creating negative social and economic consequences.[30] And though the fact of the photograph may be true, its context may not be; historical harm can occur, for example, by posting NCP alongside an allegation that the victim consented to its disclosure, or that he or she has certain sexual preferences or proclivities.[31]

In Holly Jacobs's case, Googling her name after the original images were uploaded almost exclusively brought up results of the nude photos and video.[32] As a PhD candidate who also taught undergraduate students, Jacobs worried that her professional future would be forever compromised; she legally changed her name, asking for a seal to be placed on her records, only to have the motion to seal (including both names) posted online by the county.[33] Her online identity was shattered. But the online abuse crept into her offline life when Jacobs was forced to cancel her thesis presentation for the American Psychological Association after someone reposted the nude photos alongside the date, time, and location of her talk.[34] Not only was it embarrassing to have her photos and video posted online, but prospective employers might have trouble differentiating between Holly Jacobs, PhD, and "Holly Jacobs," anonymous sex addict. How would the employer know which identity was "real"? And how likely is it that an employer would ever give her a chance to explain, instead of taking the path of least resistance and moving on to the next resume in the pile?

---

25. *See id.*
26. *See id.*
27. *See id.*
28. *See id.* at 46–47.
29. *See id.*
30. LastWeekTonight, *Online Harassment: Last Week Tonight with John Oliver (HBO)*, YOUTUBE (Jun. 21, 2015), https://www.youtube.com/watch?v=PuNIwYsz7PI [.
31. *See, e.g.*, Bekah Wells, *An Involuntary Pornstar: My Story*, WOMEN AGAINST REVENGE PORN, (Mar. 30, 2016), http://www.womenagainstrevengeporn.com/#!An-Involuntary-Pornstar-My-Story/c618/6151C735-CEEF-45B2-A175-AC3E61347B3A [https://perma.cc/UC4Q-E24F] (last visited Apr. 8, 2016).
32. *See* CITRON, *supra* note 24, at 45–47.
33. *See id.* at 48.
34. *See id.* at 49.

Jacobs founded the "End Revenge Porn" campaign in 2012,[35] and now heads a non-profit called the "Cyber Civil Rights Initiative," dedicated to "advocating for state and federal legislative" reforms.[36] Since she began her advocacy work, thirty-five states (and the District of Columbia) have initiated anti-NCP laws and many more have legislation pending.[37]

Unlike Dr. Jacobs, Anita Sarkeesian's ability to get hired does not depend on her Google search results, since she is self-employed.[38] However, like Dr. Jacobs, Sarkeesian is a victim of NCP of a slightly different variety. Sarkeesian is an avid video gamer, media critic, and activist with a popular YouTube channel called "Feminist Frequency."[39] She has garnered over 220,000 followers, posted nearly ninety YouTube videos deconstructing anti-feminist tropes in games, and her videos have tallied over twenty-six million views.[40] In 2012, when Sarkeesian launched the Kickstarter campaign to fund her now-successful YouTube channel, she received violent personal threats as well as Photoshopped pornographic images of herself.[41] These images were not versions of originals she had shared consensually, but rather what she called "image based harassment," including vulgar photo manipulation and creating pornographic or degrading drawings of rape or sexual assault with the target's likeness.[42] Just two years later, one of her videos, "Women as Background Decoration,"[43] attracted the attention of angry Internet users who sent serious enough threats that Sarkeesian fled her home as a result.[44] The threats continued, escalating to the point that Sarkeesian cancelled a talk she was scheduled to give at Utah State University after receiving a "terror threat" that promised to perpetrate "the deadliest school shooting in American history."[45]

---

35. *About*, CYBER CIVIL RIGHTS INITIATIVE, http://www.cybercivilrights.org/welcome (last visited Apr. 8, 2016).

36. *Our Mission*, CYBER CIVIL RIGHTS INITIATIVE, http://www.cybercivilrights.org/about (last visited Apr. 8, 2016).

37. *See 35 STATES + DC HAVE REVENGE PORN LAWS*, CYBER CIVIL RIGHTS INITIATIVE, https://www.cybercivilrights.org/revenge-porn-laws/ [https://perma.cc/UHQ7-5VGS] (last visited Apr. 15, 2017).

38. *Biography*, *infra* note 39.

39. *See Biography*, ANITASARKEESIAN.COM, http://www.anitasarkeesian.com/media-kit/ [https://perma.cc/73R2-A5NH] (last visited Feb. 6, 2017) [hereinafter *Biography*].

40. *See* feministfrequency, *About*, YOUTUBE, https://www.youtube.com/user/feministfrequency/about (last accessed Feb. 20, 2017).

41. *See* Amy O'Leary, *In Virtual Play, Sex Harassment Is All Too Real*, N.Y. TIMES (Aug. 1, 2012), http://www.nytimes.com/2012/08/02/us/sexual-harassment-in-online-gaming-stirs-anger.html [https://perma.cc/YMK9-ZHAB].

42. Anita Sarkeesian, *Image Based Harassment and Visual Misogyny*, feministfrequency (July 1, 2012), https://feministfrequency.com/2012/07/01/image-based-harassment-and-visual-misogyny/ [https://perma.cc/TZ6Y-S823].

43. feministfrequency, *Women as Background Decoration: Part 2 – Tropes vs. Women in Video Games*, YOUTUBE (Aug. 25, 2014), https://youtu.be/5i_RPr9DwMA.

44. *See* Anna North, *Why a Video Game Critic Was Forced to Flee Her Home*, N.Y. TIMES: OP TALK (Aug. 29, 2014, 11:34 AM), http://op-talk.blogs.nytimes.com/2014/08/29/why-a-video-game-critic-was-forced-to-flee-her-home [https://perma.cc/LN4J-WYM3].

45. *See* Soraya Nadia McDonald, *'Gamergate': Feminist video game critic Anita Sarkeesian cancels Utah lecture after threat*, WASH. POST (Oct. 15, 2014),

Luckily for Sarkeesian, she has developed a large enough public persona through her YouTube channel that it is unlikely a prospective employer would believe the Photoshopped images to be real. But this is no consolation for the vast majority of everyday victims. Sarkeesian may be less likely to suffer permanent historical harm where a quick Google search of her name yields a substantive Wikipedia page with coverage detailing her online harassment.[46] But, her reputational harm persists; Sarkeesian has had to warn her neighbors that they might see some "shady" characters around the building due to her continued notoriety.[47] Participating in a June 2017 panel at VidCon about women's online experiences, Sarkeesian was confronted by her online harassers, who sat in the front two rows filming her.[48] One of those harassers later posted a video to YouTube about their planned presence, crowing, "[w]e had a blast with this."[49] Sarkeesian herself commented on the parallels between her treatment during the "GamerGate" scandal and the increase in internet vitriol during and after the 2016 presidential election.[50]

B. American Torts & the Development of Information Privacy

The modern conception of information privacy begins with Samuel Warren and Louis Brandeis' 1890 treatise *The Right to Privacy*.[51] Warren and Brandeis were primarily concerned with reputational harm, where journalists' invasion of private and domestic life could cause emotional distress and

---

https://www.washingtonpost.com/news/morning-mix/wp/2014/10/15/gamergate-feminist-video-game-critic-anita-sarkeesian-cancels-utah-lecture-after-threat-citing-police-inability-to-prevent-concealed-weapons-at-event [https://perma.cc/4LGG-85V6].

46. *Anita Sarkeesian*, WIKIPEDIA, https://en.wikipedia.org/wiki/Anita_Sarkeesian [https://perma.cc/AS3W-8226] (last visited Apr. 8, 2016). Notably, Sarkeesian's Wikipedia page has been locked from editing by the community after it was vandalized in response to her project against anti-feminist video game tropes, which is arguably the definition of historical harm. *See* Angela Watercutter, *Feminist Take on Games Draws Crude Ridicule, Massive Support*, WIRED (June 14, 2012, 6:30 AM), http://www.wired.com/2012/06/anita-sarkeesian-feminist-games [https://perma.cc/4SGE-U8K7].

47. Todd Martens, *Video game critic Anita Sarkeesian's Web series 'Ordinary Women' to reveal little-known stories*, L.A. TIMES (Apr. 6, 2016, 4:53 PM), http://www.latimes.com/entertainment/herocomplex/la-et-hc-anita-sarkeesian-20160407-story.html [https://perma.cc/BHN7-EGWL].

48. Lindy West, *Save Free Speech From Trolls*, N.Y. TIMES: SUNDAY REV. (July 1, 2017), https://www.nytimes.com/2017/07/01/opinion/sunday/save-free-speech-from-trolls.html [https://perma.cc/E3WK-5F32].

49. Colin Campbell, *Anita Sarkeesian's astounding 'garbage human' moment*, POLYGON (June 27, 2017), https://www.polygon.com/features/2017/6/27/15880582/anita-sarkeesian-garbage-human-vidcon-interview [https://perma.cc/6QYS-YRNU].

50. *See* Anita Sarkeesian, *Understand the Power of Untapped Technology*, REFINERY29 (Jan. 19, 2017), http://www.refinery29.com/2017/01/136447/women-empowerment-trump-presidency-essays [https://perma.cc/28CR-FDYJ]; *see also* Martens *supra* note 47 at 3–4 (stating "GamerGate" "rose to prominence in mid-2014 and became an Internet hashtag championed by those who feared that any sort of cultural criticism about games . . . would result in some sort of politically correct makeover of the medium.").

51. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); *see also* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 17 (2015) ("It came to define not just the field of privacy law but also popular understandings of what privacy means.").

psychological injury.[52] At the time, the idea that a plaintiff should recover for purely emotional harm was a radical one.[53] For 125 years, lawyers have worried about the effect of new media technology on reputation, and the advent of the Internet has only accelerated these concerns. Although Warren and Brandeis have been labeled "elitists" for seeking emotional damages on behalf of the upper class, whom viewed gossip as a threat to class dignity, this traditional calculus has been upended.[54] Now the class of individuals for whom an interference with identity would be most damaging is not the elite or famous, who already occupy sizable portions of the Internet and have armies of social media publicists. While celebrities face a larger potential audience when their nude photos are uploaded to the Internet, for example, their identity rehabilitation is considerably easier due to a powerful preexisting reputation.[55] Reputational and historical harms are most damaging to the public who operates neither entirely offline nor online. Entirely offline individuals can avoid online reputational harm because their local communities are less likely to be confused—for example, an individual who has never joined Facebook can more easily argue that a Facebook account in their name is purely false. Fully online individuals with substantive and long histories of social media presence may defeat reputational and historical harms by simply continuing to create content such that negative search results decrease in proportion to in their social media presence.[56] But for those whose online presence is not deeply established prior to their victimization by NCP, it may be much more difficult to limit the negative consequences to their community reputation and historical identity. Where Warren and Brandeis worried about the reputational damage that might follow a newspaper gossip column, what happens now that Google's memory is nearly perfect? What rights, if any, does an individual have to her online identity?

Seventy years later, William Prosser refined the Warren and Brandeis conception of privacy by delineating the four distinct privacy torts commonly known today: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light; and (4) appropriation of likeness.[57] This quad-furcation of the unitary privacy right has throttled common law progression alongside technology that doesn't fit neatly into any single category, rather than

52. *See* RICHARDS, *supra* note 51, at 18.

53. *See id.*

54. *See id.* at 19.

55. Without making light of her experience, Jennifer Lawrence, for example, has fully recovered her positive reputation since her nude photos were leaked online in 2014. *See, e.g.*, Jonathan Van Meter, *Jennifer Lawrence is Determined, Hilarious, and—Above All—Real*, VOGUE (Nov. 11, 2015, 9:48 PM), http://www.vogue.com/13368193/jennifer-lawrence-december-2015-cover-hunger-games [https://perma.cc/KFZ2-6LJW].

56. *See id.*

57. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1733 (2010) (citing William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960)); RESTATEMENT (SECOND) OF TORTS § 652B (1977) (Intrusion upon Seclusion)).

allowing courts to gradually respond to changing circumstances.[58] It has also had the effect of condensing breach of privacy concerns into a checklist, rather than focusing on the specific right to be protected.[59] And because these torts have offered few protections for modern victims of NCP, [60] for example, it is difficult to see how adherence to the old regime will be flexible enough to tackle new problems.

Although "tort law is traditionally a matter of state law,"[61] the Internet is by nature multi-jurisdictional,[62] and basic principles of fairness and uniformity suggest that a federal remedy is needed. In a criminal case, venue can be problematic where, for example, the perpetrator of NCP lives in Florida but their victim lives in California.[63] The nuances of each state's online identity protection laws and long-arm statutes could also lead to vastly dissimilar results; a federal statute has the benefit of establishing a bright line rule which can be broadly applied. The Supreme Court has yet to rule on the proper jurisdictional test for personal jurisdiction over the Internet, however, the Court of Appeals for the Ninth Circuit has formulated a prototypical approach: applying *Calder v. Jones,*[64] "personal jurisdiction can be based upon: (1) intentional actions (2) expressly aimed at the forum state (3) causing harm, the brunt of which is suffered—and which the defendant knows is likely to be suffered—in the forum state."[65] This test, however, requires a level of purposeful targeting that is at odds with modern Internet usage; the

58. *See* Robert M. Connallon, *An Integrative Alternative for America's Privacy Torts*, 38 GOLDEN GATE U.L. REV. 71, 86–87 (2007) ("[T]he development of privacy-tort law has been devoid of doctrinal adjustments that would allow courts to respond to new conditions.").

59. *Id.* at 88.

60. In one of the few encouraging examples, a Colorado woman obtained a judgment against her ex-boyfriend for intentional infliction of emotional distress, but the court declined to evaluate her intrusion upon seclusion claim, finding it duplicative of the underlying facts alleged in the IIED claim. The court did, however, allow the public disclosure of private facts claim. *See* Doe v. Hofstetter, No. 11-CV-02209-DME-MJW, 2012 WL 2319052, at *7–9 (D. Colo. June 13, 2012). As an unpublished decision, however, it is of no precedential value.

61. Mary Wood, *O'Connell, A Pioneer of Insurance Law, Retires from Law School, University of Virginia School of Law* (May 10, 2012), http://content.law.virginia.edu/news/2012_spr/oconnell_retirement.htm [https://perma.cc/HML4-UQER].

62. *See, e.g.*, Dan L. Burk, *Jurisdiction in a World Without Borders*, 1 VA. J. L. & TECH. 3, 10 (1997) ("There is no centralized control of the packet routing, or for that matter, of almost any other aspect of the Internet.").

63. *See id.* at 22 ("The government may have wide latitude in deciding where to bring a prosecution against alleged on-line offenders, as the nature of the Internet is to facilitate contact between many jurisdictions, and elements of the offense may conceivably have been initiated, completed, or furthered not only where the defendant was physically located, but in all the jurisdictions that his actions electronically touched."); *see also* United States v. Rowe, 414 F.3d 271, 277–80 (2d Cir. 2005) (finding venue in the Southern District of New York proper despite the fact that defendant resided in and used his computer to post the child pornography advertisement in the Eastern District of Kentucky).

64. *See generally* Calder v. Jones, 465 U.S. 783 (1984) (establishing the "effects test" for personal jurisdiction).

65. 4A CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE § 1073 (4th ed.) (quoting Panavision Int'l., L.P. v. Toeppen, 141 F.3d 1316 (9th Cir. 1998), *modified on other grounds by* Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 443 F.3d 1199 (9th Cir. 2006)).

structure of the interconnected Internet makes it impossible to control where all of a user's data goes, short of staying off the Internet entirely.[66] To establish a federal tort-like remedy for interference with online identity, it is necessary to return to the historical unitary cause of action and center it around the protected right: online identity.[67]

C. Criminal Law: Non-Consensual Pornography and Cyberstalking

Civil remedies do not stand alone. Criminal penalties have also been levied against perpetrators of interference with online identity. The Philippines was the first country to criminalize NCP in 2009.[68] In the United States, California is considered a leader in online criminal legislation and anti-NCP laws[69]; New Jersey, however, was both the first state to criminalize NCP and the first to convict for its distribution.[70] As of this writing, thirty-five states and the District of Columbia have anti-revenge porn laws.[71] Of those, New Jersey's statute has been rarely used,[72] and California's statute classifies revenge porn as a disorderly conduct misdemeanor.[73] Notably, the District of Columbia's law makes publication of NCP a felony punishable by up to three years in prison, though it also includes a misdemeanor subsection.[74] Only California has amended its state constitution to include a right to privacy.[75]

---

66. *See* Burk, *supra* note 62, at 50.

67. *See* Cristina Carmody Tilley, *Rescuing Dignitary Torts from the Constitution*, 78 BROOK. L. REV. 65, 70 (2012) ("Historically, the dignitary torts were treated as a unitary cause of action, protecting a key component of personal security—namely, interests in individual personality. The fracturing of this interest into distinct torts has marginalized the underlying interest they protect.").

68. Mary Anne Franks, *The Fight Against Digital Abuse: The View from the US*, WOMEN'S AID (Dec. 15, 2015 12:25 PM), http://www.womensaid.ie/16daysblog/2015/12/15/the-fight-against-digital-abuse-the-view-from-the [https://perma.cc/E8C2-QVNX].

69. *See generally California Online Privacy Protection Act*, CONSUMER FED'N CAL.: EDUC. FOUND., https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/ [https://perma.cc/LU2U-UP27] (last accessed Apr. 2, 2017).

70. *See* Paul J. Larkin, Jr., *Revenge Porn, State Law, and Free Speech*, 48 LOY. L.A. L. REV. 57, 94–95 (2014); *see also* State v. Parsons, 2011 WL 6089210 (N.J. Super. Ct. App. Div. Dec. 8, 2011).

71. CYBER CIVIL RIGHTS INITIATIVE, *supra* note 35.

72. *See* Paul J. Larkin, Jr., *Revenge Porn, State Law, and Free Speech*, 48 LOY. L.A. L. REV. 57, 95 (2014) (noting the statute was also used against the roommate of Tyler Clementi, the Rutgers University student who committed suicide after the roommate live broadcasted Tyler and another man having consensual sex).

73. *See* CAL. PENAL CODE § 647(j)(4) (West 2017).

74. D.C. CODE § 22–3053 (West 2015); *see also* Keith L. Alexander, *D.C. man becomes first to be convicted under District's new revenge porn law*, WASH. POST (Apr. 19, 2017), https://www.washingtonpost.com/local/public-safety/dc-man-becomes-first-to-be-convicted-under-districts-new-revenge-porn-law/2017/04/19/2e6ab4ca-2516-11e7-b503-9d616bd5a305_story.html?utm_term=.44dd6f5a2603 [https://perma.cc/J5UC-NHPQ].

75. *See* CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").

This state constitutional right has been extended to some aspects of digital privacy, but its development has been far from straightforward.[76] While promising, this approach is necessarily limited to California residents or to individuals with deep enough pockets to pursue litigation in the venue of the perpetrator. And although California recently announced its first conviction under its anti-NCP statute,[77] the piecemeal protection of various rights afforded by state tort law is, at best, insufficiently flexible to adapt to changing technologies. As Holly Jacobs's experience demonstrates, local state and federal law enforcement is often unfamiliar with or unwilling to research the remedies already available to victims.[78]

In contrast to the patchwork state approach, there is no federal anti-revenge porn law. United States House Representative Jackie Speier was set to introduce a federal bill in late 2015,[79] but it has yet to cross the House floor. Previous attempts to legislate at the federal level have faced strong opposition from free speech advocates, and on fundamental issues like whether NCP should even be considered a criminal act.[80] Given the ambivalence in even progressive political circles,[81] which are more likely to support a bill, it seems unlikely that such legislation will be taken up seriously for some time. However, the realistic pace of a historically unproductive Congress should not factor into the equation of whether these harms *should* be redressed. A federal statute criminalizing behavior that impermissibly interferes with an online identity would effectively deter several types of offenses that plague Internet use in society today.

Despite the lack of federal action to criminalize NCP, cyberstalking and child pornography are established federal crimes whose underlying statutes may provide a model for a federal statute concerned with online identity.[82]

---

76. *See* White v. Davis, 533 P.2d 222, 233–35 (Cal. 1975) (looking to text of voter advocate brochures to determine whether constitutional amendment was intended to extend to information privacy).

77. *See* Veronica Rocha, *'Revenge porn' conviction is a first under California law*, L.A. TIMES, (Dec. 4, 2014, 5:00 PM), http://www.latimes.com/local/crime/la-me-1204-revenge-porn-20141205-story.html [https://perma.cc/9SRH-6PFM].

78. *See* CITRON, *supra* note 24, at 41.

79. *See* Lydia Wheeler, *Lawmaker eyes 'revenge porn' crackdown*, HILL (Jul. 15, 2015 6:00 AM), http://thehill.com/regulation/247954-lawmaker-eyes-revenge-porn-crackdown [https://perma.cc/A4VX-SULY].

80. *See* Kaveh Waddell, *Bill to Criminalize Revenge Porn Coming After Recess*, NAT'L J. (Aug. 12, 2015, 1:00 AM) (quoting an ACLU staff attorney as saying: "[w]e don't use criminal law to remedy humiliation"), https://www.nationaljournal.com/s/70267 [https://perma.cc/W8CT-UGZB].

81. *Compare* Mary Anne Franks, *The ACLU's Frat House Take on 'Revenge Porn'*, HUFFINGTON POST, http://www.huffingtonpost.com/mary-anne-franks/the-aclus-frat-house-take_b_6980146.html [https://perma.cc/535L-Z234] (Apr. 1, 2015 1:23 PM) (criticizing the ACLU's opposition to state revenge porn legislation), *with* Lee Rowland, *VICTORY! Federal Judge Deep-Sixes Arizona's Ridiculously Overbroad 'Nude Photo' Law*, ACLU (July 10, 2015 6:45 PM), https://www.aclu.org/blog/speak-freely/victory-federal-judge-deep-sixes-arizonas-ridiculously-overbroad-nude-photo-law [https://perma.cc/URL8-SR6P] (defending ACLU's stance on "opposing laws that chill or criminalize protected speech, even when we condemn the conduct that well-meaning legislators are trying to target").

82. *See generally* Naomi Goodno, *Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 MO. L. REV. 125, 127–28 (2007).

The Violence Against Women Reauthorization Act of 2013 ("VAWA") amended the federal cyberstalking statute to include harsher sentences.[83] However, the Supreme Court struck down the part of the original VAWA that allowed victims to sue their attackers for damages in federal court.[84] The Court reasoned that "[t]he Constitution requires a distinction between what is truly national and what is truly local."[85] But since 2000, when *United States v. Morrison* was decided, Internet access has permeated the country to an extent unanticipated by Chief Justice Rehnquist's opinion.[86] The federal Circuits have disagreed on whether the Internet is more properly described as a channel or instrumentality of interstate commerce, or both, under the Commerce Clause.[87]

Most of these decisions have arisen in the context of child pornography cases, in which the defendants have used the Internet to store or obtain criminal images.[88] At the very least, cyberstalking and child pornography statutes and case law provide a helpful blueprint for identifying constitutional questions that should be addressed in any proposed legislation.

D. Good but Not Good Enough: Copyright Law, the Communications Decency Act, and the Fair Credit Reporting Act

As the law currently stands, there is no comprehensive statutory structure to protect online identity; rather, one who experiences this kind of harm must look to the federal laws to see if a remedy exists. Recent scholarship on anti-NCP statutes and online harms have focused on a variety of well-established precedents to import into the new technology.[89] Even popular news programs, such as the HBO show "Last Week Tonight with

83. *Compare* 18 U.S.C. § 2261(b) (2000), *with* 18 U.S.C. § 2261(b)(6) (2012) (adding a provision punishing violation of injunction, restraining order, or no-contact order with not less than one year's imprisonment).

84. *See* United States v. Morrison, 529 U.S. 598, 598 (2000).

85. *See id*. at 617.

86. *See* generally Diane McGimsey, *The Commerce Clause and Federalism after Lopez and Morrison: The Case for Closing the Jurisdictional-Element Loophole*, 90 CAL. L. REV. 1675, 1719 (2002) ("[T]he growth of communications networks across the United States has greatly increased the likelihood that any activity will involve some line crossing and thus potentially permits all activities to be regulated under the Court's current approach to the jurisdictional element [of Commerce Clause jurisprudence].").

87. *Compare* United States v. MacEwan, 445 F.3d 237, 253 (3d Cir. 2006) ("We therefore hold that the Internet is both a channel and instrumentality of interstate commerce and that Congress can regulate the downloading of child pornography over the Internet under 18 U.S.C. § 2252A(a)(2)(B) even if the transmission never crossed state lines."), *with* United States v. Hornaday, 392 F.3d 1306, 1311 (11th Cir. 2004) ("The internet is an instrumentality of interstate commerce.").

88. *See, e.g.*, *MacEwan*, 445 F3d. at 253; *Hornaday*, 392 F.3d at 1311 .

89. *See, e.g.*, Citron & Franks, *supra* note 7, at 346–347 (drawing on First Amendment doctrine); Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 67 (2009) (arguing for free speech protection); Derek E. Bambauer, *Exposed*, 98 MINN. L. REV. 2025, 2052–56 (2014) (proposing copyright law as a framework).

John Oliver," have discussed the applicability of copyright remedies to NCP, for example.[90]

Copyright law, as a potential method of combatting NCP, has the distinct advantage of being rooted in the federal Constitution and in a well-established statutory scheme.[91] It therefore might appear to offer an attractive alternative system of control over the use of information without violating the First Amendment.[92] In practice, however, copyright law leaves much to be desired, because website owners often ignore takedown requests, betting correctly that few victims will have the financial resources to go through protracted litigation.[93] The victim of NCP also may not have been the photographer, and therefore not the copyright owner.[94] Even if the victim took the photograph herself, the victim must first register new photos of her body with the United States Copyright Office in order to claim ownership of the content.[95]

More intangibly, reliance on copyright characterizes the harm as a violation of a property right, rather than a dignitary tort.[96] And, crucially, even a successful takedown notice cannot "put the genie back in the bottle" and prevent the same content from being reposted on another website.[97] Even if a victim owns the copyright and makes a timely demand for removal, Google will delink NCP, but will also provide a disclaimer, stating: "In response to a complaint we received under the US Digital Millennium Copyright Act, we have removed X result(s) from this page. If you wish, you may read the DMCA complaint that caused the removal(s) at [the website]," providing a direct link to the original content.[98]

Regardless of its shortcomings, copyright law is a quintessential example of one way the law regulates the flow of information in a way society feels is reasonable.[99] And, crucially, copyright even restricts some First Amendment rights.[100] Copyright protections may even be too strong, but the existence of a large body of copyright law makes it arguable that creating a protection for online identity, which could be seen as an individual's fundamental intellectual property, is not unprecedented. And copyright does

---

90. LastWeekTonight, *supra* note 30.

91. *See* U.S. CONST. art. I, § 8, cl. 8; Digital Millennium Copyright Act of 1998, 17 U.S.C. § 1201 *et seq.* (2012).

92. *See* SOLOVE, *supra* note 16, at 185.

93. *See* Citron & Franks, *supra* note 7, at 359–60.

94. *See id.*

95. *See* Mitchell A. Matorin, *In the Real World, Revenge Porn is Far Worse Than Making It Illegal*, TALKING POINTS MEMO (Oct. 18, 2013, 6:00 AM), http://talkingpointsmemo.com/cafe/our-current-law-is-completely-inadequate-for-dealing-with-revenge-porn [https://perma.cc/2JMN-XXWN].

96. *See* Citron & Franks, *supra* note 7, at 357 (citing Cristina Carmody Tilley, *Rescuing Dignitary Torts from the Constitution*, 78 BROOK. L. REV. 65, 65 (2012)).

97. *Id.* at 360.

98. *See* Matorin, *supra* note 95.

99. *See* SOLOVE, *supra* note 16, at 185 ("Control in the privacy context is seen as outlandish or impossible. Copyright law demonstrates otherwise.").

100. *See id.* at ch.7 n.77 (citing to Eldred v. Ashcroft, 537 U.S. 186, 190 (2003) ("Copyright's protections are so strong that even the First Amendment right to freedom of expression yields before them.")).

offer a way around another potential barrier to recovery for victims of NCP: section 230 of the Communications Decency Act.[101]

The Communications Decency Act ("CDA") was passed on February 1, 1996, in response to conservatives' concerns about Internet pornography.[102] Despite its origin as an attempt to protect children from "indecent" material on the Internet,[103] the statute has been broadly interpreted.[104] Though the Supreme Court struck down the vast majority of section 230 in a landmark case, the immunity provisions of section 230 that exempt secondary posters of content from liability remain.[105] Specifically, section 230 of the CDA has been applied by some courts to allow purposeful republishing by website owners of known illegal material (in some cases, including NCP) while effectively enjoying legal immunity.[106] State criminal law is also preempted by section 230, leaving a sizable loophole for intermediary posters, even in states with more stringent standards of liability.[107]

Accordingly, a federal statute aimed at protecting online identity might more appropriately be modeled after the Fair Credit Reporting Act. The Fair Credit Reporting Act ("FCRA") was adopted in 1970,[108] with an express goal of protecting consumer privacy.[109] To that end, the statute contains two provisions allowing private citizens to sue: one for willful non-compliance, and one for negligent non-compliance.[110] A recent case, however, which is again pending before the Ninth Circuit on remand from the Supreme Court,[111] has highlighted a potential constitutional standing issue with Congress's attempt to create private causes of action under the FCRA;[112] the plaintiffs

---

101. *See* Citron & Franks, *supra* note 7, at 359 ("[Section] 230 does not immunize websites from federal intellectual property claims.").

102. *See* Amanda L. Cecil, *Taking Back the Internet: Imposing Civil Liability on Interactive Computer Services in an Attempt to Provide an Adequate Remedy to Victims of Nonconsensual Pornography*, 71 WASH. & LEE L. REV. 2513, 2538–39 (2014).

103. *See* Reno v. ACLU, 521 U.S. 844, 868 (1997) ("[T]he purpose of the CDA is to protect children from the primary effects of 'indecent' and 'patently offensive' speech . . . .").

104. *See* Danielle Keats Citron & Neil Richards, *Can and Should Perez Hilton Be Held Liable for Reposting Celebrities' Private Nude Photos Without Their Consent?*, FORBES (Sept. 3, 2014, 4:41 PM), http://www.forbes.com/sites/daniellecitron/2014/09/03/can-and-should-perez-hilton-be-held-liable-for-reposting-celebrities-private-nude-photos-without-their-consent/#2715e4857a0b6a10e553327e [https://perma.cc/BS5E-DGTQ].

105. *See Reno*, 521 U.S. at 868 (1997); *see also* Citron & Franks, *supra* note 7, at 7.

106. *See* Citron & Franks, *supra* note 7, at 8.

107. Bambauer, *supra* note 89, at 2088 (citing 47 U.S.C. § 230(e)(3)).

108. Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1128 (codified as amended at 15 U.S.C. § 1681 et seq. (2012)).

109. *See* United States v. Bormes, 133 S. Ct. 12, 15 (2012).

110. *See generally* James Lockhart, Annotation, *Remedies Available in Private Action Under §§ 616 and 617 (15 U.S.C.A. §§ 1681n, 1681o) of Fair Credit Reporting Act—Other than Attorney's Fees*, 20 A.L.R. Fed. 2d 509 (2007) (compiling and analyzing cases that explore the types of remedies, other than attorneys' fees, available under the FCRA's two private causes of action); *see also* 15 U.S.C. §§ 1681n, 1681o.

111. *See* Robins v. Spokeo, Inc., 742 F.3d 409, 412 (9th Cir. 2014), *vacated*, 136 S. Ct. 1540 (2016).

112. *See* Brief for Petitioner Spokeo, Inc. at 36, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13–1339).

alleged that under the "statutory" cause of action, a plaintiff need not show actual harm to have standing, and that the false information about Robins itself was a willful violation of the statute.[113]

E. Jurisdiction and the Internet

The most compelling benefit of a federal statute cementing a federal cause of action and remedy is a simple one: uniformity and fairness. By nature, the Internet is multi-jurisdictional.[114] The need for a federal statute to combat malicious interference with online identity is apparent when considering the alternatives. Although tort law may appear attractive, it has traditionally been a matter of state discretion, which poses inherent problems to any comprehensive legislative remedy.

Questions of personal jurisdiction have arisen as a particularly problematic area of Internet law, and the varying approaches taken by federal courts around the country only serve to contribute to this general feeling of confusion.[115] Some federal courts, in analyzing whether personal jurisdiction exists over Internet activity, require the forum state to be the focal point of the defendant's allegedly slanderous or libelous statements, *and* that there be evidence of the website being accessed by residents of the forum state other than the plaintiff.[116] Does unauthorized access to a victim's Facebook account constitute "minimum contacts"? What about where the harm is felt? Many courts still apply a version of the *Calder* test, which leads to, at best, inconsistent results when applied to the Internet.[117] When NCP is posted to a website hosted on servers located exclusively in Indiana, hypothetically, what jurisdiction would a California court have over the contents? Will every court agree with the Northern District of Illinois that "[t]he fact that cyber-space was the medium for inflicting harm is of no moment"?[118]

F. Standing

In early 2016, the Supreme Court released its opinion in *Spokeo, Inc. v. Robins*, which focused on whether Congress has the power to grant a plaintiff standing to sue in federal court by statute, the FCRA, without a showing of traditional concrete harm.[119] Standing consists of three elements: 1) an injury-

113. *See Robins*, 742 F.3d at 412.

114. *See, e.g.*, WRIGHT ET AL., *Supra* note 65; *see also* Burk, *supra* note 62, at 21–24.

115. *See, e.g.*, Diane McGimsey, *The Commerce Clause and Federalism after Lopez and Morrison: The Case for Closing the Jurisdictional-Element Loophole*, 90 CAL. L. REV. 1675, 1719–20 (2002) (discussing holding in United States v. Kammersell, 196 F.3d 1137 (10th Cir. 1999), that a Utah resident who sent his girlfriend a threatening instant message via AOL, which traveled through a server in Virginia, was sufficient to satisfy "interstate commerce" requirement of federal statute).

116. *See* WRIGHT ET AL., *Supra* note 65.

117. *See id.*

118. *See* Info. Techs. Intern., Inc. v. ITI of N. Fla., Inc., 2001 WL 1516750, at *7–8 (N.D. Ill. 2001).

119. *See* Brief for Petitioner Spokeo, Inc. at 36, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13–1339); *see also* Spokeo Inc. v. Robins, 136 S. Ct. 1540, 1544–45 (2016).

in-fact, 2) which is fairly traceable to the defendant's conduct, and 3) is likely to be redressed by judicial decision.[120] Because injury-in-fact is an Article III constitutional requirement, Congress cannot grant standing to a plaintiff merely through statutory fiat.[121] The FCRA establishes, in sections 1681n and 1681o, that failure to comply with certain minimum standards gives rise to a cause of action.[122] Robins argued that the statutory violation was harm in and of itself.[123] In terms of devising an online identity statute, this problem should be avoided by writing into the statute itself that damage to an online identity is a cognizable harm. A major barrier to potential lawsuits is that the current trends in data breach law, for example, do not allow for lawsuits when economic injury cannot be shown.[124] Typically, most courts do not find a threat of future harm to be sufficient injury to confer standing upon a plaintiff.[125] The Supreme Court's doctrine of Article III standing requires "injury in fact," which is both "concrete and particularized," and "not conjectural or hypothetical".[126] The Court attempted to clarify the "concrete and particularized" requirement in *Spokeo* by explaining that "particularized" injury means it "must affect the plaintiff in a personal and individual way."[127] While particularization is necessary to establish injury in fact, it is not sufficient; the injury must also be concrete.[128] In the words of the Court, a concrete injury must "actually exist," but that is not necessarily synonymous with "tangible."[129] In dicta, the Court explained the risk of real harm can, in circumstances like libel or slander *per se*, satisfy the concreteness requirement.[130] In such cases, the plaintiff "need not allege any *additional* harm beyond the one Congress has identified."[131] This Note will therefore argue that the interference with online identity itself is one of those cases where a technical violation would result in a cognizable injury-in-fact, as specifically defined in the proposed federal statute, and should be sufficient to provide standing, even under the current *Spokeo* framework.[132]

120. *See* 136 S.Ct. at 1547 (citing Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992)).

121. *See* 136 S.Ct. at 1547–48.

122. *See* 15 U.S.C. §§ 1681n, 1681o.

123. *See* Brief of Respondent Thomas Robins at 15, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13–1339).

124. *See generally In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1211–12 (N.D. Cal. 2014); Carlsen v. GameStop, Inc., 112 F. Supp. 3d 855, 860 (D. Minn. 2015) (pending appeal).

125. *See generally* Brief for Petitioner Spokeo, Inc. at 36, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13–1339).

126. *Spokeo Inc.*, 136 S. Ct. at 1548.

127. *See id.* (citations omitted).

128. *See id.*

129. *See id.* at 1549.

130. *See id.*

131. *See id.*

132. The case is currently on remand to the Ninth Circuit, and may return to the Supreme Court for another round. *See* Allison Grande, *Spokeo Points 9th Circ. to Sister Court's Denials*, LAW360 (Dec. 2, 2016), https://www.law360.com/appellate/articles/868587/spokeo-points-9th-circ-to-sister-courts-denials.

IV. ANALYSIS & PROPOSAL: TOWARD A FEDERAL STATUTE

A federal statute would be the most effective remedy for the current state of affairs, where the Supreme Court has yet to fully confront questions of Internet jurisdiction, speech, and online-to-offline harm.[133] Though several states have made efforts to create or expand a right to online identity, they have largely sought to accomplish this through modest expansions of traditional privacy-tort law.[134] Law will never develop simultaneously with technology;[135] but as our technology becomes rapidly more complex, it is essential that any new legislation leave substantial breathing room for novel concepts.

The federal statute proposed here includes both civil and criminal elements. Tort law lends a useful framework to this statute, and constitutional torts can similarly create a federal cause of action.[136] After first laying out a substantive proposal, this section of the Note will then discuss arguments in favor of, and in opposition to, such a statute, and finally will conclude by disposing of likely constitutional challenges.

A. Malicious Interference with Online Identity

This Note proposes establishment of a federal tort and a federal crime for malicious interference with online identity. The ideal formulation for the tort of malicious interference with online identity is similar to civil battery[137]: 1) an act, uploading the information to the Internet; 2) with intent to harm the victim or their online identity; and contact, where information that reaches the victim is harmful or offensive to a reasonable person,[138] or which the perpetrator would have reason to know would be harmful or offensive to that particular person (e.g., NCP uploaded by a former lover). Crucially, like the FCRA, and as discussed in *Spokeo*, the cause of action must be specific, concrete, and identify the misinformation itself as the harm against which the

133. *See* discussion *supra* Section III.E–F.

134. *See, e.g.*, Connallon, *supra* note 58, at 77–82 (reviewing modern state privacy-tort law in the context of the Restatement Prosser-style four privacy rights). *Compare* MASS. GEN. LAWS ANN. ch. 214, § 1B (West 2015) ("A person shall have a right against unreasonable, substantial or serious interference with his privacy."), *with* White v. Davis, 13 Cal. 3d 757, 775 (1975) (en banc) ("[T]he amendment is intended to be self-executing, i.e., that the constitutional provision, in itself, creates a legal and enforceable right of privacy for every Californian." (interpreting Art. 1 § 1 of California State Constitution)).

135. *See* ROBERT J. KLOTZ, THE POLITICS OF INTERNET COMMUNICATION 136 (2004) ("One fundamental challenge of cyberlaw is that technology moves faster than the law.").

136. *See* Tilley, *supra* note 67, at 76–77 ("Several theories of the Ninth Amendment suggest that the rights protected by the dignitary torts may be among those 'retained by the people' and thus shielded from disparagement relative to those enumerated in the Constitution.").

137. *See, e.g.*, W. Va. Fire & Cas. Co. v. Stanley, 216 W.Va 40, 51 (2004) ("An actor is subject to liability to another for battery if (a) he acts intending to cause a harmful or offensive contact with the person of the other or a third person, or an imminent apprehension of such a contact, and (b) a harmful contact with the person of the other directly or indirectly results." (citing RESTATEMENT (SECOND) OF TORTS § 13 (1965)).

138. *See, e.g.*, *infra* note 157 (cat picture subreddit versus porn star).

statute should protect.[139] Further, civil damages should be measured similarly to the intentional infliction of emotional distress tort, including, but not limited to, physical injury, lost wages (with a duty to mitigate), reimbursement for psychotherapy, and costs of issuing takedown notices. The proposed federal tort statute should thus state: any person who, knowing he is not authorized or privileged to do so, intentionally discloses identity information about another that he knew, or should have known, would harm the individual's online identity, with the intent to cause or attempt to cause substantial emotional distress as a result, shall be liable to the individual victim for actual damages, such amount of punitive damages as the court may allow, and in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

Practically speaking, American tort law often requires a plaintiff to have two things: physical injury, and deep pockets. Interference with online identity, by its very nature, will frequently have no physical injury—until or unless humans have avatars walking the physical world in their stead.[140] But by establishing a federal cause of action that need not show physical injury, similar to sections 1681n and 1681o of the FCRA,[141] Congress should recognize that the injury-in-fact *is* the damage to the individual's online identity. Further, class actions are not without precedent, especially in the FCRA context,[142] and would alleviate the need for an individual plaintiff to bear the costs of the entire litigation. Given the heavy burden on a plaintiff tackling a civil and criminal case simultaneously, class actions would significantly lessen that burden and provide an avenue to obtain judgment against serial bad actors.

As with data privacy statutes, the most important section of this legislation will be the Definitions. Clearly defining "online identity" and "malicious interference" is essential. As a threshold matter, what should "online identity" mean? Implicitly, the phrase assumes that there is something inherently distinct about an online identity. The statute should define online identity as a comprehensive overview of information about an individual,

---

139. *See* Transcript of Oral Argument at 21, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13–1339), https://www.supremecourt.gov/oral_arguments/argument_transcripts/2015/13-1339_j5fl.pdf [https://perma.cc/6ZQY-BJA6].

140. This is not especially far-fetched. *See, e.g.*, Victoria Thorp, *Beam store on University Avenue gives Palo Alto a glimpse into a robotic future*, PALO ALTO PULSE (Mar. 2, 2015), http://www.paloaltopulse.com/2015/03/02/beam-store-on-university-avenue-gives-palo-alto-a-glimpse-into-a-robotic-future [https://perma.cc/78TW-UUYE]; *see also President Obama greets Alice Wong via Beam during the ADA's 25th Anniversary*, BEAM:BLOG (July 21, 2015), http://blog.suitabletech.com/2015/07/21/president-obama-beam [https://perma.cc/H7EF-G29K].

141. *See* 15 U.S.C. §§1681n, 1681o.

142. *See generally In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 851 F. Supp. 2d 1040, 1047 (S.D. Tex. 2012); Soutter v. Equifax Info. Servs., LLC, 307 F.R.D. 183, 195 (E.D. Va. 2015).

information which is "continuous and dynamic," and which can be ascribed to the individual by others.[143]

To simplify, in the following example "the individual" will be referred to as "N." Identity information can be directly within N's control (e.g., a personal Facebook profile, to which she has a right to exclude others);[144] indirectly within her control (e.g., a photograph taken by N's Facebook friend in which N is tagged); or entirely outside her control (e.g., a Craigslist solicitation posting uploaded by an ex-boyfriend).[145] The federal statute should not limit online identity to the sources with which the public is currently familiar, such as Google and Facebook, but should extend to any website or platform that hosts, links to, compiles or processes an individual's personal information. Platforms should not be directly liable for hosting information about N which later turns out to be false, as that would result in a profoundly overbroad chilling effect on speech.[146] But this must be balanced against N's interest in recovering against, for example, an ex-boyfriend "P", who posts nude photographs to a shared Facebook group.[147] It is not difficult to imagine how, to proving liability, a plaintiff may have difficulty attributing the unconsented-to content to a particular perpetrator—e.g., if Facebook expeditiously removes the original photos, but duplicates continue to be hosted on a subdomain of the social media site reddit (also known as a "subreddit"); an individual plaintiff without very deep pockets would effectively be estopped from asserting her rights altogether.[148] Ideally, a malicious user should not be able to escape liability by simply reposting the content to another web host.[149] It is crucial to recognize that this statute aims

---

143. *See* Elad Oreg, *Right to Information Identity*, 29 J. MARSHALL J. COMPUTER & INFO. L. 539, 580–81 (2012).

144. This Note does not address the applicability of terms like Personally Identifiable Information ("PII"), agreeing with Professor Ohm that PII is unworkable, ever-expanding, and unsuccessful at defining what information will identify an individual. *See* Ohm, *supra* note 57, at 1742; *see also id.* at 1765–1768 (listing "five factors for assessing the risk of privacy harm": "data handling techniques," "private versus public release," "quantity," "motive," and "trust").

145. *See* DeeDee Correll, *Former boyfriend used Craigslist to arrange woman's rape, police say*, L.A. TIMES (Jan. 11, 2010), http://articles.latimes.com/2010/jan/11/nation/la-na-rape-craigslist11-2010jan11 [https://perma.cc/57DA-EP5E] (providing example of identity information outside the control of the individual).

146. *See* SOLOVE, *supra* note 16, at 182 ("A line must be drawn at cyberspace; once the information is out on the Internet, those subsequently discussing and disseminating it should not be liable. To conclude otherwise would seriously chill the freewheeling and lively discussion that rapidly erupts across the blogosphere.").

147. *See, e.g.*, Andrew Liptak, *The US military is investigating a secret Facebook group that spread naked pictures of service women*, VERGE (Mar. 5, 2017), https://www.theverge.com/2017/3/5/14820242/military-investigating-secret-facebook-group-marines-united-service-women [https://perma.cc/7VSM-82N6].

148. *See, e.g.*, Mitchell A. Matorin, *In the Real World, Revenge Porn is Far Worse Than Making It Illegal*, TALKING POINTS MEMO (Oct. 18, 2013, 6:00 AM), http://talkingpointsmemo.com/cafe/our-current-law-is-completely-inadequate-for-dealing-with-revenge-porn [https://perma.cc/97EV-3ZXM].

149. This is a classic and ongoing problem with hosting sites like The Pirate Bay, which envisions itself as a "hydra", alluding to its unstoppable rebirth as soon as one site is shut down. *See, e.g.*, Emil Protalinski, *The Pirate Bay is not down: Domain redirect problem has an easy fix*, VENTUREBEAT (May 24, 2015, 8:25 AM) http://venturebeat.com/2015/05/24/the-pirate-bay-is-not-down-domain-redirect-problem-has-an-easy-fix [https://perma.cc/2J9L-46YQ].

not to control the behavior of third-party consumers of N's information,[150] or of websites that may repost the original content. Rather, it aims to give the victim "decision-making authority about oneself, from which one can presumptively exclude others."[151]

Identifying information should not be strictly defined by Personally Identifiable Information ("PII"), as in data breach statutes.[152] Doing so would not only ensure that the statute would be vulnerable to rapid changes in technology,[153] but it also would enshrine a reductive understanding of what constitutes identity.[154] Instead of specifying particular characteristics to consider, the statute should be triggered when a reasonable person would be misled by the interference with the victim's identity. It is key to focus the law on the victim's ability to control the dissemination of identity information, rather than on the perpetrator's. As Professor Oreg notes, in impersonation law, certain jurisdictions only recognize the offense if there is intent to defraud, which exculpates perpetrators who impersonate a victim in order to harm the victim, and not others.[155] This is exactly the type of harm this statute is designed to rectify.

Factors to consider in an analysis of whether a reasonable person would confuse the two versions of an online identity (e.g., Dr. Holly Jacobs, PhD versus "Holly Jacobs", sex addict) should include: trustworthiness of the source;[156] ability to identify the content poster (anonymous posters are

---

150. As a moral issue, accessing such sensitive information may be repugnant, but a federal statute should refrain from addressing it due to First Amendment concerns. *See* SOLOVE, *supra* note 16, at 182 ("[O]nce the information is on the Internet, however, it would be impractical and problematic to hold liable others beyond the person who initially placed it there."). As a practical matter, a large part of modern internet culture involves online "stalking" one's acquaintances. *See, e.g.*, Carol Roth, *The Right Way to 'Stalk' People Online*, ENTREPRENEUR (July 15, 2014), http://www.entrepreneur.com/article/235080 [https://perma.cc/X2VU-UDEV].

151. *See* Daniel R. Ortiz, *Privacy, Autonomy, and Consent*, 12 HARV. J.L. & PUB. POL'Y 91, 92 (1989).

152. *See, e.g.*, Paul M. Schwartz and Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 82 N.Y.U. L. REV. 1814, 1845–47 (2011); *see also* Ohm, *supra* note 57, at 1742 (comparing the constant need to amend the definition of PII to a game of whack-a-mole).

153. For example, many state legislatures have pending bills to supplement data breach statutes' definition sections with obsolete additions. In New Jersey, for example, the State Legislature introduced A.B. 1239 in 2014, which proposed new restrictions on "magnetic-stripe data" of credit or debit cards. By October 2015, banks had moved to "chip-and-PIN" cards where customer data is stored only in an embedded microchip (and not in the magnetic strip). *See* A.B. 1239, NJ ASSEMBLY, http://www.njleg.state.nj.us/2014/Bills/A1500/1239_I1.HTM [https://perma.cc/GMX6-VHEF] (last visited Apr. 10, 2016); *see also* Kim Zetter, *Hacker Lexicon: What are Chip and PIN Cards?*, WIRED (Apr. 15, 2015, 9:00 AM), http://www.wired.com/2015/04/hacker-lexicon-chip-pin-cards [http://www.wired.com/2015/04/hacker-lexicon-chip-pin-cards].

154. *See* Oreg, *supra* note 143, at 585 ("There is a temptation to attempt to objectively determine the importance of different aspects of a person's life which constitute his identity . . . [but] [u]ltimately, any attempt to grade the aspects of a person's life using categorical classifications will be simplistic . . . .").

155. *See id.* at 587.

156. The trustworthiness of a source should consider the purpose of the hosting site; i.e., a post on Backpage, a website preferred by prostitutes for advertising, is far less trustworthy

generally less trustworthy than named posters); similarity to the victim's existing online profile; and the victim's subjective belief in the distortion's importance (e.g., N might not bring litigation to protect her identity from impersonation on a subreddit about cat pictures, but would find it more troubling to have her head Photoshopped onto the body of a porn star).[157] This test may also be satisfied by circumstantial evidence, if, for example, a victim can show a series of job interviews that were suddenly cancelled after a prospective employer initiated a Google search or background check that yielded misinformation, or if the general public and members of the community report knowledge of the perpetrator's misinformation.[158] But the individual need not show specific economic harm; so long as the harm shown satisfies Article III standing requirements,[159] the harm is the misinformation itself.[160]

B. Criminal Interference with Online Identity

Federal laws against cyberstalking and state laws against NCP are both useful tools to protect online identity, but they do not accomplish the expressive justice purpose that the proposed federal statute would. Take the example of Hunter Moore, the "most hated man on the Internet," who created Is Anyone Up?, a website that hosted and disseminated revenge porn images.[161] In contrast to Noe Iniguez, the first defendant to be convicted under California's state anti-revenge porn law and who received a year's prison sentence,[162] Moore and an accomplice were federally indicted.[163] He eventually pled guilty to one count of unauthorized access to a protected computer and one count of aggravated identity theft, and was sentenced to

---

than Facebook, Craigslist is less trustworthy than Google+, Facebook is less trustworthy than a verified Twitter, etc.

157. *See id.* at 588 ("[A]n offense reflecting a true commitment to the right of identity would grade the gravity of the offense and its surrounding circumstances in accordance with the importance of the stolen identity and the degree of its distortion, and not just according to the severity of the other offense made possible by the impersonation.").

158. *See* discussion *supra* Section III.A.

159. Again, *Spokeo* is back in the Ninth Circuit on remand, and leaves questions about what exactly is required for standing in such a case. Amy Howe, *Opinion analysis: Case on standing and concrete harm returns to the Ninth Circuit, at least for now*, SCOTUSBLOG (May 16, 2016, 6:45 PM), http://www.scotusblog.com/2016/05/opinion-analysis-case-on-standing-and-concrete-harm-returns-to-the-ninth-circuit-at-least-for-now/ [https://perma.cc/F3L6-T2FP].

160. Justice Ruth Bader Ginsburg's dissent in the latest iteration of *Spokeo* provides some support for this approach. *See* Spokeo, Inc. v. Robins, 136 S. Ct. at 1556 (Ginsburg, J., dissenting) ("I therefore see no utility in returning this case to the Ninth Circuit to underscore what Robins' complaint already conveys concretely: Spokeo's misinformation "cause[s] actual harm to [his] employment prospects.").

161. Jessica Roy, *Revenge-Porn King Hunter Moore Indicted on Federal Charges*, TIME (Jan. 23, 2014), http://time.com/1703/revenge-porn-king-hunter-moore-indicted-by-fbi [https://perma.cc/E2JC-UTEW].

162. *See* Rocha, *supra* note 77.

163. Roy, *supra* note 161.

two-and-a-half years in federal prison.[164] Had there been a federal criminal penalty for malicious interference with online identity, as herein proposed, Iniguez and Moore's sentences may have been similar, but expressive justice would be much better served. As Professors Danielle Keats Citron and Mary Anne Franks have noted, while Moore's conviction is cause for celebration, it does not make existing law any more successful at protecting an individual's identity: "[t]he fact that one revenge porn site owner allegedly broke numerous federal laws in running a revenge porn website does not change the fact that *he is facing no charges for publishing the content itself* . . . ."[165] In the absence of a federal remedy tailored to these specific societal concerns, the power of expressive justice is lost. The ends do not justify the means.

Moreover, the most salacious and well-publicized examples of interference with N's online identity typically cross over into criminal law. Here, the issue is not simply whether a reasonable person could tell the difference between the "real" N and the "doppelganger" N, but whether the perpetrator himself has breached a societal norm that deserves prosecution. And, crucially, a federal statute, with both civil and criminal enforcement mechanisms, provides a two-fold authority that encompasses both "judgment-proof" defendants and those practically immune to criminal prosecution (i.e., sites protected by section 230 of the CDA).

The existing federal cyberstalking statute, 18 U.S.C. section 2261(a), requires the perpetrator to engage in a "course of conduct" intended to harass or intimidate a victim;[166] a "course of conduct" is defined as "a pattern of conduct composed of [two] or more acts, evidencing a continuity of purpose."[167] However, this ignores the reality of viral sharing on the Internet today. A single upload may be shared thousands of times, reaching an audience of millions, and yet would not likely qualify as a "course of conduct."[168] Accordingly, the proposed federal statute would criminalize even the initial act of posting, but scale the penalties in accordance with the audience reached and harm caused. Taking elements from California's more narrow approach and New Jersey's broader one,[169] the federal statute would provide: it is a crime for an actor, knowing he is not authorized or privileged to do so, to intentionally disclose identity information about another that he knew, or should have known, would harm the individual's online identity, with the intent to cause or attempt to cause substantial emotional distress as a result. A knowledge requirement regarding consent is crucial in order to protect reporters and news media; it is the reporter's job to inquire into where

164. Abby Ohlheiser, *Revenge porn purveyor Hunter Moore is sentenced to prison*, WASH. POST (Dec. 3, 2015), https://www.washingtonpost.com/news/the-intersect/wp/2015/12/03/revenge-porn-purveyor-hunter-moore-is-sentenced-to-prison [https://perma.cc/M6W2-4PVR].

165. *See* Citron & Franks, *supra* note 7, at 368 (emphasis added).

166. *See* Citron & Franks, *supra* note 7, at 365–66.

167. *See* 18 U.S.C. § 2266 (2012).

168. *See* Citron & Franks, *supra* note 7, at 365–66.

169. *Compare* CAL. PEN. CODE § 647(j)(4) (2015) (listing specific sexual acts covered by statute), *with* N.J. STAT. ANN. § 2C:14–9 (2004) (criminalizing unconsented disclosure of reproduction of images showing "an act of sexual penetration or sexual contact").

the information comes from. There should also be a specific carve-out to defeat a "heat of passion" mitigating theory as in voluntary manslaughter: "adequate provocation" shall be no defense. The definition of online identity for criminal infractions, therefore, should be substantially similar to the civil one. This emphasizes the holistic intent of the statute to protect the integrity of online identity.

C. Arguments Against Creating a Right of Online Identity: Constitutional Challenges

The clearest obstacle to the proposed federal statute is the First Amendment's Free Speech Clause. There is evidence to suggest that the Supreme Court would not look favorably upon a federal statute of such breadth.[170] However, because this proposed statute is narrowly tailored, rejects the binary public/private conception of privacy and seeks to regulate a category of speech between historically circumscribed child pornography and defamation, it passes constitutional muster.

1. The First Amendment

Privacy interests clash directly with First Amendment jurisprudence because privacy is not limited to controlling falsehoods, as in defamation cases.[171] The essence of a right to privacy in one's online identity is effectively a right to exclude, but it is not absolute.[172] In order to avoid invalidation by the First Amendment, the federal statute must be narrowly tailored to focus on the individual's right to speak, on the Internet if she so chooses, about her own life, and to prevent others from interfering with the "intellectual property" of her identity.[173] The statute should not be evaluated under a strict scrutiny standard because the kind of speech the statute seeks to restrict is most analogous to defamation, and therefore is outside the scope of the First Amendment altogether.[174] But even if it were evaluated under strict scrutiny, this proposal should prevail.

---

170. *See, e.g.*, Bambauer, *supra* note 89, at 2087–88 ("Under Chief Justice John Roberts, the Supreme Court has been especially rigorous about evaluating[, under the First Amendment,] laws that also made strong claims to tangible harms, from bans on crush videos involving the torture of animals to limits on violent video games due to negative effects on minors, to tort liability for the deliberate infliction of emotional distress upon a deceased veteran's family during his funeral procession, and to limits on government funding based on the need to reduce prostitution as a means of fighting the spread of HIV/AIDS." (citations omitted)).

171. *See* SOLOVE, *supra* note 16, at 126–27 (2007).

172. *See id.* at 170 ("[Privacy] involves establishing control over personal information, not merely keeping it completely secret.").

173. *See id.* at 134.

174. *See id.* at 186–87 ("The right to withdraw from the public gaze at such times as a person may see fit, when his presence in public is not demanded by any rule of law, is also embraced within the right of personal liberty."(citing Pavesich v. New England Life Ins. Co., 50 S.E. 68, 70 (Ga. 1905) (the first decision to recognize the appropriation tort)). These cases developed before the Supreme Court had established the now-canonical system of levels of scrutiny; *Pavesich* grounded the right to control individual disclosure in the Fourteenth

The First Amendment does not protect every kind of speech. For example, it does not extend to speech used to "engage in fraud," "to form and advance conspiracies," or "to solicit criminal acts."[175] It also does not bar the imposition of tort liability for defamatory statements.[176] Similarly, punishing online speech that maliciously interferes with another's identity should not be considered an abridgement of the freedom of speech.[177] The trouble with First Amendment doctrine, however, is that the greater does not always include the lesser power.[178] NCP falls somewhere between child pornography, which the Supreme Court has held is entirely outside the First Amendment,[179] and traditional defamation law, which the Court has struggled to update to modern standards.[180] Defamation and libel law were both well-established at the time of the First Amendment's ratification, making a strong originalist argument for why they should still apply in an Internet context.[181] Supreme Court precedent suggests that it will view the Internet as the next frontier of communications technology, and will likely apply the same standards of First Amendment scrutiny.[182] In dicta, the Court also acknowledged the problem of the "community standards" test as applied to the Internet: "[T]he 'community standards' criterion as applied to the Internet means that any communication available to a nationwide audience will be judged by the

---

Amendment's "liberty" interest. 50 S.E. at 70 ("Liberty includes the right to live as one will, so long as that will does not interfere with the rights of another or of the public. One may desire to live a life of seclusion; another may desire to live a life of publicity; still another may wish to live a life of privacy as to certain matters, and of publicity as to others.").

175. Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 U.C.L.A. L. REV. 1149, 1171 (Apr. 2005) (citing to KENT GREENAWALT, SPEECH, CRIME, AND THE USES OF LANGUAGE 40 (1989)).

176. GREGORY E. MAGGS & PETER J. SMITH, CONSTITUTIONAL LAW: A CONTEMPORARY APPROACH 994 (3d ed. 2015) (citing Beauharnais v. Illinois, 343 U.S. 250, 266 (1952)).

177. Richards, *supra* note 175, at 1171.

178. *See, e.g.*, R.A.V. v. City of St. Paul, 505 U.S. 377, 401 (1992) (White, J., concurring in the judgment) ("It is inconsistent to hold that the government may proscribe an entire category of speech because the content of that speech is evil, but that the government may not treat a subset of that category differently without violating the First Amendment; the content of the subset is by definition worthless and undeserving of constitutional protection.").

179. *See* New York v. Ferber, 458 U.S. 747, 765 n. 18 (1982) ("Today, we hold that child pornography . . . is unprotected speech subject to content-based regulation. Hence, it cannot be underinclusive or unconstitutional for a State to do precisely that.").

180. *Compare* Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 758–59 (1985) ("[S]peech on 'matters of public concern' . . . is 'at the heart of the First Amendment's protection.'"), *with* Snyder v. Phelps, 562 U.S. 443, 454 (2011) (finding public concern present where the Westboro Baptist Church picketed an individual soldier's funeral due to the "overall thrust and dominant theme of Westboro's demonstration" speaking to broader public issues); *see also Phelps*, 562 U.S. at 465–471 (Alito, J., dissenting) ("[A]lthough this court has not decided the question, I think it is clear that the First Amendment does not entirely preclude liability for the intentional infliction of emotional distress by means of speech. . . . The First Amendment allows recovery for defamatory statements that are interspersed with nondefamatory statements on matters of public concern . . . .").

181. *See, e.g.*, Chaplinsky v. New Hampshire, 315 U.S. 568, 571–72 (1942) ("There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to pose any Constitutional problem. These include . . . the libelous . . . .").

182. *See* Reno v. ACLU, 521 U.S. 844, 870 (1997).

standards of the community most likely to be offended by the message."[183] Therefore, the proposed federal statute must establish a firm baseline upon which potential perpetrators, prosecutors, and judges can rely.

Even if the Supreme Court were to determine this kind of restriction on speech to be content-based, it would still survive strict scrutiny because the proposed statute is narrowly tailored to advance the government's interest in protecting the health and safety of its citizens, as well as their ability to contribute to and participate in the national economy.[184] It is crucial to differentiate the proposed statute from other content-based restrictions on speech because this proposal does not seek to punish the *underlying speech*.[185] The statute is not aimed at preventing nude photographs from being taken, but *only* at preventing their dissemination, with scienter, via a particularly far-reaching mode of publication (i.e., the Internet).[186] Nonetheless, consent to share with a wider audience should be an absolute defense. As Professor Daniel Solove explains: "[w]e want to limit the flow of information, not stop it completely."[187] Consent to share should therefore be evaluated by degree. Consent to share between intimate partners, or even on some parts of the Internet like a support community, is quintessentially distinct from consent to share with the entire Internet. Finally, as a policy matter, criminalizing malicious dissemination of NCP will actually encourage *more* speech. In the current legal landscape, rather than risk being victimized, individuals are often told to simply stop engaging in the underlying speech.[188] Criminalizing NCP thus recognizes that consensual sexual photography is not a disappearing trend,[189] and will actually encourage more expression by removing some of the fear of exposure beyond the intended audience.

---

183. *See id.* at 877–78.

184. *See* Boos v. Barry, 485 U.S. 312, 321 (1988); Sable Commc'ns of Cal., Inc., v. FCC, 492 U.S. 115, 126 (1989) ("The Government may, however, regulate the content of constitutionally protected speech in order to promote a compelling interest if it chooses the least restrictive means to further the articulated interest.").

185. *Boos*, 485 U.S. at 336 ("[A]ny restriction on speech, the application of which turns on the content of the speech, is a content-based restriction regardless of the motivation that lies behind it.").

186. In one of the few existing court challenges to a state anti-NCP law, a Vermont court grappled with this problem. *See* State v. Van Buren, No. 1144-12-15Bncr (Vt. Super. July 1, 2016). Finding NCP to not fall into the obscenity category of unprotected speech, the court concluded the statute failed the least restrictive means test because, as a hypothetical, the statute would also "criminalize disclosure by a party who never had any relationship with complainant and who received such unsolicited sexual photographs and decided to disclose them to convince complainant not to send any more or out of anger for being the recipient." The proposed statute is narrowly tailored to punish only disclosure with intent to harm, and therefore should survive a similar challenge.

187. *See* SOLOVE, *supra* note 16, at 184.

188. *See, e.g.*, Helena Horton, *Revenge porn: 'Grow up' and stop taking naked photos to avoid becoming a victim, say police*, TELEGRAPH (Feb. 18, 2016), http://www.telegraph.co.uk/women/life/revenge-porn-grow-up-and-stop-taking-naked-photos-to-avoid-becom/ [https://perma.cc/FB7R-3LQM].

189. *See, e.g.*, Ashley Welch, *How popular is sexting? The numbers may surprise you*, CBS NEWS (Aug. 10, 2015), http://www.cbsnews.com/news/sexting-popular-among-adults-study-finds [https://perma.cc/9FRA-BLAY].

V. CONCLUSION

There will always be tension between the right to control one's identity and the right to free expression. Because the Internet is a relatively new technology—one that promises to bring long-lasting change—Congress is the appropriate body to put forward a federal law that addresses changing norms. The harms of NCP and the difficulty of extricating one's online identity from one's offline identity illustrate the clear benefits of a bright-line statutory rule. Yet the First Amendment can, and should, allow for some limited and narrowly tailored government regulation of online speech. Therefore, an omnibus law that includes both civil and criminal penalties would deliver a comprehensive castigation of those bad actors who seek to permanently damage others' online identities.