

2017

The Victim May Forgive, but the Internet Will Never Forget: The Need to Adopt a Variant on the Right to be Forttten as a Remedy for Nonconsensual Pornography

Holly M. Coppens

Follow this and additional works at: http://scholarship.shu.edu/student_scholarship



Part of the [Law Commons](#)

Recommended Citation

Coppens, Holly M., "The Victim May Forgive, but the Internet Will Never Forget: The Need to Adopt a Variant on the Right to be Forttten as a Remedy for Nonconsensual Pornography" (2017). *Law School Student Scholarship*. Paper 915.
http://scholarship.shu.edu/student_scholarship/915

**THE VICTIM MAY FORGIVE, BUT THE INTERNET WILL NEVER FORGET: THE
NEED TO ADOPT A VARIANT ON THE RIGHT TO BE FORGOTTEN AS A REMEDY
FOR NONCONSENSUAL PORNOGRAPHY**

Holly M. Coppens

In response to the growing expansion of the internet and a desire to keep this growth sustained, Congress passed the Communications Decency Act (“CDA”) of 1996, and along with it, Section 230.² §230(c) holds, “no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”³ §230 essentially safeguards internet service providers “from claims arising out of content created by third-parties.”⁴ The initial purpose of §230 of the CDA was to quell the fears of internet service providers concerned about liability for postings made by users of their websites.⁵ The panic stemmed from the New York Supreme Court decision in *Stratton Oakmont, Inc. v. Prodigy Services Co.*, holding an internet service provider liable for comments posted by a third-party user of the website.⁶ The court found Prodigy liable for two main reasons: (1) Prodigy publicly stated it controlled the content on its site and (2) Prodigy used software programs designed to control content on its online “bulletin boards.”⁷ The Supreme Court of New York ultimately

² Jenna K. Stokes, Article, *The Indecent Internet: Resisting Unwarranted Internet Exceptionalism in Combating Revenge Porn*, 29 Berkeley Tech. L.J. 929, 932 (2014).

³ Communications Decency Act, 47 U.S.C.S. §230 (1996).

⁴ Brian J. McBrearty, *Who’s Responsible? Website Immunity Under the Communications Decency Act and the Partial Creation or Development of Online Content*, 82 Temp. L. Rev. 827, 828 (2009).

⁵ Stokes, *supra* note 1.

⁶ *Stratton Oakmont v. Prodigy Servs. Co.*, No. 31063/94, 1995 N.Y. Misc. LEXIS 229, at *17 (N.Y. Sup. Ct. May 24, 1995).

⁷ *Id.* at *10.

relied on the concept of agency to connect Prodigy with its users, opening up all internet service providers to similar suits under an agency relationship.⁸

After the §230 of the CDA came into existence, courts began to hold in the complete extreme to *Stratton*: internet services providers should be given full immunity, unless specific conditions are met.⁹ The courts apply a three-part test to find immunity for internet services providers: “(1) the party seeking immunity is a provider or user of an interactive computer service, (2) the claim treats the party seeking immunity as the publisher or speaker of the disputed content, and (3) the claim is based on content produced by another information content provider.”¹⁰ More concisely, the website claiming immunity as a defense needs to show the content wholly came from a third-party.¹¹ In *Zeran v. Am. Online, Inc.*, the United States Court of Appeals for the Fourth Circuit held the District Court did not err in accepting AOL’s §230 defense.¹² The Court of Appeals broadened the language of §230, stating “§230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party.”¹³ §230 makes no direct mention of immunities, but through interpretation courts have expanded the CDA to, perhaps somewhat unintended, heights.¹⁴ The Court of Appeals for the Fourth Circuit additionally emphasized congressional intent to encourage internet service providers to “self-regulate” information posted by third party users.¹⁵ The Court of Appeals recognized a need to hold differently than the *Stratton* court, because the liability could deter service providers from self-regulation.¹⁶

⁸ *Id.* at *17.

⁹ *See generally* Stokes, *supra* note 1 at 934.

¹⁰ *McBrearty, supra* note 3 at 832.

¹¹ *See generally Id.* at 833.

¹² *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 335 (1997).

¹³ *Id.* at 330.

¹⁴ CDA, *supra* note 2.

¹⁵ *Zeran, supra* note 8 at 331.

¹⁶ *Id.*

Following similar logic, the Court of Appeal of California, Second Appellate District found MySpace immune from claims under §230 in *Doe II v. MySpace Inc.*¹⁷ The Court of Appeal examined cases across all circuits and found a “general consensus to interpret [§]230 immunity broadly.”¹⁸ The case involved a female minor lured by another user to his home and subsequently assaulted by him.¹⁹ The claims stemmed from entirely third-party to third-party communication, but the plaintiff ultimately wanted to hold MySpace liable as a content provider.²⁰ Even though MySpace played a more active role in terms of what content users were required to post, the Court of Appeal ultimately held it “was not an information content provider subject to liability under section 230.”²¹

Similarly, in the development of Section 230 immunity, the United States Court of Appeals for the Sixth Circuit granted immunity in *Jones v. Dirty World Entm’t Recordings LLC*.²² The case involved anonymous postings of defamatory comments on TheDirty.com website.²³ The Court of Appeals laid out a test of “material contribution to the alleged illegal content” for determining when an internet service provider would be held liable as an internet content provider.²⁴ The Sixth Circuit Court of Appeals found: “(1) the defendants are interactive service providers, (2) the statements at issue were provided by another information content provider, and (3) Jone’s claim seeks to treat the defendants as a publisher or speaker of those statements, the CDA bars Jone’s claims.”²⁵

¹⁷ *Doe II v. MySpace, Inc.* 175 Cal. App. 4th 561, 575 (2009).

¹⁸ *Id.* at 572.

¹⁹ *Id.* at 565.

²⁰ *Id.* at 574.

²¹ *Id.* at 575.

²² *Jones v. Dirty World Entm’t Recordings LLC*, 755 F.3d 398, 417.

²³ *Id.* at 403.

²⁴ *Id.* at 410.

²⁵ *Id.* at 417.

Most recently in the case against Hunter Moore and his website Isanyoneup.com, a perpetrator of both promoting and uploading nonconsensual pornography took a plea of two years jail time and a \$2,000 fine.²⁶ Moore pleaded guilty to hacking computers to steal nude photos, which he posted without consent and with identifiable information attached.²⁷ Moore's sentence did not revolve around §230 protections, but instead the government charged him with a felony for hacking. Moore was sentenced to two years in prison, but on charges unrelated to his posting of nonconsensual pornography.²⁸ The Moore case is an example of when immunity wouldn't be given to a website operator, even though Moore's transition from an internet service provider from an internet content provider did not affect the outcome of the case.

As the cases above reveal, courts have been hard-pressed to hold internet service providers liable for content posted by third-parties, and immunities have been extended to “web hosting services, email service providers, commercial websites (i.e. Amazon and eBay), individual and company websites, Internet dating services, privately-created chat rooms, and Internet access points in copy centers and libraries.”²⁹ Victims of nonconsensual pornography may feel less confident in bring claims against website operators knowing courts often find §230 immunity applies, forcing new remedies to be sought. Although the court in *Zeran* emphasized congress's desire for self-regulation by website operators, this grand notion has fallen by the wayside. The current in-flux, or maybe lack thereof, of cases involving nonconsensual pornography or revenge porn cast a bright light on how §230 and a scarcity in self-regulation are failing victims of such crimes.

²⁶ See generally Brian Feldman, *Revenge-Porn Mogul Hunter Moore is Going to Prison for Two Years*, NY Mag (Dec. 3, 2015, 12:21PM), <http://nymag.com/following/2015/12/hunter-moore-is-going-to-prison.html>.

²⁷ *Id.*

²⁸ Lizzie Plaugic, *Revenge porn website operator Hunter Moore sentenced to 30 months in prison: He will also have to pay a \$2,000 fine*, The Verge (Dec. 3, 2015, 12:16PM), <http://www.theverge.com/2015/12/3/9843038/hunter-moore-revenge-porn-is-anyone-up-prison-sentence>.

²⁹ Stokes, *supra* note 1 at 934.

Part I of this note will address the “revenge porn phenomenon,” examining the origins, ways cases generally arise, and how the crime should ultimately be labeled. Additionally, Part I will discuss the lasting impact revenge porn postings have on its victims and how it is a seemingly never ending offense. Part II of this note will analyze current legal remedies available in US Courts for victims of nonconsensual pornography. The discussion will begin first with an examination of criminal laws, next with an analysis of tort claims, and finally copyright actions will be described. Part III will examine the “Right to Be Forgotten” under European Union law and the case that gave victory to Privacy rights over Speech rights. An analysis as to the feasibility and practicability of the EU system will be conducted. Part IV will address how the “Right to Be Forgotten” could work under the current US legal system as the best remedy for victims of nonconsensual pornography. The response of website operators in the US to revenge porn and nonconsensual pornography claims will also be discussed in comparison to Section 230 of the CDA. Part V will conclude and recommend a variant on the “Right to Be Forgotten” should be brought to the US as a means to aid victims of nonconsensual pornography.

I. The Revenge Porn “Phenomenon”

As the Internet becomes the most used form of communication across the world, the ease of accessibility and the lack of policing have caused many issues of late, one being “revenge porn” or nonconsensual pornography. Revenge porn entails the online posting of “nude or sexually explicit photos or videos” of a former partner without his or her consent.³⁰ The term “revenge porn” is not entirely inclusive of the definition, prompting some to broaden the term to

³⁰ Luke Fiedler, Article, *Public Shaming in the Digital Age: Are Criminal Laws the Most Effective Means to Regulate Revenge Porn?*, 34 Loy. L.A. Ent. L. Rev. 155, 157 (2014). See also Taylor Linkous, Article, *It’s Time for Revenge Porn to Get a Taste of its Own Medicine: An Argument for the Federal Criminalization of Revenge Porn*, 20 Rich. J.L. & Tech. 14, *3 (2014).

“nonconsensual pornography.”³¹ Revenge porn conjures up images of “angry exes with intimate photos or videos of their former significant others [who] weaponize that media after the breakup by uploading it to the internet.”³² Nonconsensual pornography is a more encompassing term defined as “the distribution of sexually graphic images of individuals without their consent.”³³ Nonconsensual pornography generally arises in one of three scenarios: “(1) nonconsensual photography or video recording, (2) consensual photography or video recording that is later stolen, [or] (3) consensual photography or video recording that is intentionally transmitted to an individual.”³⁴ Examining the ways in which victims bring claims involving nonconsensual pornography, using a more general term helps to change the view that the only postings that matter are those between scorned partners. For the purposes of this note, the term nonconsensual pornography will be used as it is more encompassing of the realities affecting victims of such crimes.

Although lately discussed as a “phenomenon,” revenge porn has been around for years.³⁵ In 2008, there were numerous blogs and websites specifically created for users to post humiliating nudes of ex-partners.³⁶ To compound the injuries caused by revenge porn, posters generally attach the victim’s name, address, links to social media pages, and other personal identifiers.³⁷ The effects of these actions can be seen within days of the initial post, as the images posted can command the top search results for a given victim’s name.³⁸ Upon discovering the postings, victims generally

³¹ Cyber Civil Rights Initiative, *FAQ’s, End Revenge Porn* (2015), <http://www.endrevengeporn.org/faqs/>.

³² Stokes, *supra* note 1 at 929.

³³ Cyber Civil Rights Initiative, *supra* note 27.

³⁴ Stokes, *supra* note 1 at 929.

³⁵ Linkous, *supra* note 29 at *3.

³⁶ *Id.*

³⁷ *Id.* at *4. See also Layla Goldnick, Note, *Coddling the Internet: How the CDA Exacerbates the Proliferation of Revenge Porn and Prevents a Meaningful Remedy for its Victims*, 21 *Cardozo J.L. & Gender* 583, 585 (2015).

³⁸ Cyber Civil Rights Initiative, *supra* note 30.

experience “a debilitating loss of self-esteem, crippling feelings of humiliation and shame, discharge from employment, verbal and physical harassment, and even stalking” by other Internet users who view the images.³⁹ The Internet poses a particular problem for victims of revenge porn as it has a permanent quality thus far unseen in other modes of communication.⁴⁰

Many critics of revenge porn laws have turned to victim blaming to downplay the lasting effects of the posted images.⁴¹ The creator of the site, End Revenge Porn, also a victim, spoke out on the issue stating, “I let my guard down and trusted [my ex-boyfriend] in ways that I would not with others. I shared intimate moments with him because we were in a relationship. We should not blame the victim. It’s like blaming someone who was raped and saying that they should not have worn a certain outfit.”⁴² Revenge porn threatens legitimate harm to victims including solicitations on social media pages, loss of jobs, or a life full of fear that employers, friends, and family will discover the images.⁴³ The importance of not victim blaming leads directly into the issue at hand: revenge porn needs to be taken seriously with adequate remedies provided through the legal system.

II. Current Legal Remedies for Victims of Revenge Porn in the US

A. Bringing Tort Actions to Compensate Victims

One method of redressing harms from nonconsensual pornography involves Tort claims brought by victims to target specific harms: damaged reputations, privacy invasions, and intentionally inflicted emotional distress.⁴⁴ Within these overarching harms lay claims of

³⁹ Paul Larkin, Jr., Article, *Revenge Porn, State Law, and Free Speech*, 48 Loy. L.A. L. Rev. 57, 65 (2014).

⁴⁰ *Id.* at 60.

⁴¹ Danielle Keats Citron, *Hate Crimes in Cyberspace* 49, 49 (Harvard University Press 2014).

⁴² *Id.*

⁴³ Amanda Levendowski, *Our Best Weapon Against Revenge Porn: Copyright Law? Most revenge-porn victims took the photographs themselves- meaning that they own the rights to those selfies*, The Atlantic (Feb. 4, 2014), <http://www.theatlantic.com/technology/archive/2014/02/our-best-weapon-against-revenge-porn-copyright-law/283564/>.

⁴⁴ Danielle Keats Citron, *supra* note 40 at 120.

defamation, intentional infliction of emotional distress, or public disclosure of private information.⁴⁵ Many proponents of employing tort law as a redress for harms incurred by victims view claims of intentional infliction of emotional distress as the most flexible option, and consequently the best option.⁴⁶ Intentional infliction of emotional distress allows a victim to bring an action against both the actual poster of revenge porn and the site used to perpetuate the links to the uploaded images.⁴⁷ Revenge porn also fits neatly into the definition of intentional infliction of emotional distress since it falls under “truly outrageous conduct, of a kind especially calculated to cause serious mental and emotional disturbance”.⁴⁸ The motivation behind posting intimate images of an ex-partner is degradation and humiliation.⁴⁹ Defamation claims are also readily available for victims because they involve situations where an individual has “besmirched” the victim’s good name or reputation.⁵⁰ Additionally, under a public disclosure of private information claim, a defendant would have to pay damages for publicizing private, non-newsworthy information.⁵¹

Although perhaps the most widespread in terms of covered offenses, tort law also bears a heavy burden on the victim bringing the suit.⁵² Civil actions are “costly, time-consuming, and often draw further attention to the offending material.”⁵³ Since tort claims are a civil action, it is up to the victim to pay for the suit.⁵⁴ If the victim wins, it may be moot since the defendant will not

⁴⁵ Linkous, *supra* note 29 at *8. See also Goldnick, *supra* note 36 at 608 (“In addition to invasion of privacy claims, many cases brought by victims of revenge porn allege defamation and libel...”).

⁴⁶ Linkous, *supra* note 29 at *9.

⁴⁷ *Id.*

⁴⁸ Larkin, *supra* note 38 at 78.

⁴⁹ Stokes, *supra* note 1 at 947.

⁵⁰ Larkin, *supra* note 38 at 78.

⁵¹ Danielle Keats Citron, *supra* note 40 at 121.

⁵² Cyber Civil Rights Initiative, *supra* note 30.

⁵³ *Id.*

⁵⁴ Linkous, *supra* note 29 at *9.

likely able to pay the damages.⁵⁵ This simply means that the defendant is judgment-proof and there is little reason for bringing a civil suit if damages cannot and will not be paid.⁵⁶ Furthermore, tort claims such as harassment and stalking do not generally apply to individuals who upload revenge porn because there is no repeat of the offense upon which the claim rests, unless the perpetrator posts numerous times and satisfies the requisite standard.⁵⁷

Defendants can also raise the defense of consent to refute any tort claims against them.⁵⁸ The claim of consent, which is a complete defense, easily applies to self-portraits (“selfies”) taken by the victim.⁵⁹ Defendants in tort suits may also assert truth to defamation claims as a defense, since the victim is not misrepresented or distorted in the images.⁶⁰ Regardless of the defenses that can be asserted to tort claims, victims do not receive the ultimate remedy: a takedown of the images posted.⁶¹ Tort suits lead to high costs, provide little if any redress, and fail to adequately dissuade individuals from uploading revenge porn.⁶²

B. Creating Criminal Laws to Dissuade Future Revenge Porn Postings

In the US, the most common answer proposed for victims is enhancing old or creating new criminal laws. Since national attention has been placed on revenge porn as a crime worth punishing, twenty-six states have adopted some form of criminal revenge porn laws.⁶³ State legislators cite multiple reasons why criminal laws have been a go to for combating revenge porn: (1) criminal laws are a better deterrence against future nonconsensual uploads of intimate images;

⁵⁵

Id.

⁵⁶ Cyber Civil Rights Initiative, *supra* note 30.

⁵⁷ Levendowski, *supra* note 42.

⁵⁸ Larkin, *supra* note 38 at 80.

⁵⁹ *Id.* at 81.

⁶⁰ *Id.*

⁶¹ *See generally* Linkous, *supra* note 29 at *9.

⁶² *Id.*

⁶³ Cyber Civil Rights Initiative, 26 States Have Revenge Porn Laws, End Revenge Porn (2015), <http://www.endrevengeporn.org/revenge-porn-laws/>.

(2) criminal suits are less expensive for victims; and (3) criminal laws specifically target those who post the images, generally the ex-partner.⁶⁴

Although it is the trendiest option for remedying revenge porn victims, criminal laws face many challenges.⁶⁵ New Jersey was the first state to employ a law against revenge porn, but it did so almost accidentally.⁶⁶ New Jersey's law states,

An actor commits a crime of the third degree if, knowing that he is not licensed or privileged to do so, he photographs, films, videotapes, records, or otherwise reproduces in any manner, the image of another person whose intimate parts are exposed or who is engaged in an act of sexual penetration or sexual contact, without the person's consent and under circumstances in which a reasonable person would not expect to be observed.⁶⁷

The New Jersey Attorney General's office explained, "the language of the statute is quite broad and arguably applies to allow prosecution of an individual in a 'revenge porn' situation."⁶⁸ The New Jersey criminal law manages to strike a balancing between being broad enough to include revenge porn scenarios, while not being too broad as to affect an individual's freedom of speech rights.

State criminal laws, if written properly, can be effective in handing down punishments against posters of nonconsensual pornography. The central issue lies in whether the punishments are actually helpful for the victims.⁶⁹ In 2013, Florida legislators failed to pass a criminal revenge porn because it required the posting to include the victim's personal information to be held

⁶⁴ Fiedler, *supra* note 29 at 162.

⁶⁵ *Id.* at 163.

⁶⁶ *Id.* at 164.

⁶⁷ N.J.S. § 2C:14-9 (2004).

⁶⁸ Fiedler, *supra* note 29 at 164.

⁶⁹ See Generally Sarah Jeong, *Revenge Porn is Bad. Criminalizing it is Worse*, Wired (Oct. 28, 2013, 9:30AM), <http://www.wired.com/2013/10/why-criminalizing-revenge-porn-is-a-bad-idea/>.

criminal.⁷⁰ Many critics believed this was too narrow a scope for the law and would provide an “out” from criminal liability for individuals who upload revenge porn.⁷¹

There are several critiques of state laws criminalizing revenge porn. First, overbroad criminal laws can easily infringe upon an individual’s first amendment rights.⁷² For example, California’s first attempt at a revenge porn criminal law made it a “disorderly conduct for a defendant to take intimate and confidential recordings, such as photos or videos, and then distribute them to intentionally cause serious emotional distress to the victim.”⁷³ Reporters who linked to nonconsensual materials in the course of their work could be found guilty under the original California law.⁷⁴ While suits may not be brought against all individuals ensnared in the dragnet of the over-broad law, the possibility that reporters and bloggers could be brought as defendants reveals an infringement of free speech rights.⁷⁵

Second, the ultimate issue of the images being on the internet is not solved through criminal trials. Criminal trials place defendants on the stand with a possibility of facing various sentencing options, including jail time, but this does not aid the victim in having his or her nude image viewed by millions of internet users. It may bring emotional satisfaction for the victim to get revenge against the defendant for his or her actions, but the harm is still occurring with every click of the mouse and link to the nonconsensual post.

Third, criminal laws also reveal bigger flaws in the justice system, where police may not recognize a cyber-crime for what it truly is: a crime.⁷⁶ Revenge porn, in certain instances, violates

⁷⁰ Fiedler, *supra* note 29 at 165.

⁷¹ *Id.*

⁷² *Id.*

⁷³ *Id.* at 166.

⁷⁴ Jeong, *supra* note 68.

⁷⁵ *See Generally Id.*

⁷⁶ Fiedler, *supra* note 29 at 170.

existing criminal laws such as blackmail, stalking, or voyeurism, but police may not be equipped with the knowledge to regard online behavior the same way as an tangible crime scene.⁷⁷

In the US, as of recently, there has been much support and speculation regarding the creation of federal criminal laws against revenge porn. Many advocates note that the immunities granted in §230 of the CDA do not affect federal criminal laws, as it does state criminal law.⁷⁸ §230(e) provides that the Act shall have no effect on criminal law.⁷⁹ Additionally, federal laws could be the ultimate deterrent for posting revenge porn, as well as provide victims with better resources for proving their claims.⁸⁰

Overall, however, criminal laws still need to strike a balance between to extremes: (1) the laws are so overbroad it leads to unconstitutional results and (2) the laws are too narrow and thus ineffective for the majority of nonconsensual pornography cases.⁸¹ Regardless of whether the legislator makes a law criminalizing revenge porn at the state or the federal level, the victim's remedy is not complete. The images remain on the internet for anyone to see from the moment they are posted to anytime in the foreseeable future.

C. Using Copyright Laws to Remove Nonconsensual Postings

Congress enacted the Communications Decency Act of 1996 (“CDA”) as a way to ensure the growth of the internet, free from encumbrances and obstacles that would dissuade the technological expansion.⁸² Congress believed that the internet would hold “unimaginable benefits,” which it has, but these benefits have parallel burdens.⁸³ The CDA's immunity for

⁷⁷

Id.

⁷⁸

Id. at 176.

⁷⁹

CDA, *supra* note 2.

⁸⁰

Id. at 174.

⁸¹

Stokes, *supra* note 1 at 941.

⁸²

Goldnick, *supra* note 36 at 599.

⁸³

Id.

website hosts and operators has proved to bear the heaviest of burdens on victims of revenge porn.⁸⁴ Websites, such as Google or Yahoo, who hold links to revenge porn are immune from suit if the host played no actual role in the promulgation of the images.⁸⁵ Generally, search engine websites and the like are simply “passive transmitters of information provided by others.”⁸⁶ The CDA is what has allowed the internet to be what it is for so long; without it, there would be no user posts, blogs, comments, and social networks.⁸⁷

In order to bypass the immense protections accorded website hosts and operators under the CDA, victims have turned to copyright law to have material taken down.⁸⁸ Under the Digital Millennium Copyright Act (“DMCA”), victims of revenge porn have used the Online Copyright Infringement Liability Limitation Act (“OCILLA”) to request internet service providers take down images they own.⁸⁹ Some, but not all, intimate images taken in a relationship are “selfies” or self-portrait type pictures.⁹⁰ Approximately 80 percent of all revenge porn images posted fall under this category.⁹¹ This gives the victim ownership of the image as a copyright that can be enforced under the DMCA in the form of a take-down notice.⁹² Under the CDA there is a safe-harbor provision for internet service providers that allows them to field take-down notices before actually being

⁸⁴ See *Id.* (“This immunity serves as a massive roadblock on the route to ending revenge porn and finding a way to remedy the injuries inflicted on upon its victims, by largely exempting the websites and operators that host the revenge porn material from liability”).

⁸⁵ *Id.* (“However, this immunity remains intact only if the [internet service provider] was not also acting as an [information content provider] of the contested content: if the webhost or operator somehow created or materially changed the content of the posts, that [internet service provider] might also be deemed an [information content provider] of that content”).

⁸⁶ Linkous, *supra* note 29 at *10.

⁸⁷ Caitlin Dewey, *How Copyright Became the Best Defense Against Revenge Porn*, The Washington Post (Sep. 8, 2014), <https://www.washingtonpost.com/news/the-intersect/wp/2014/09/08/how-copyright-became-the-best-defense-against-revenge-porn/>.

⁸⁸ *Id.*

⁸⁹ Goldnick, *supra* note 36 at 611.

⁹⁰ Linkous, *supra* note 29 at 10.

⁹¹ Levendowski, *supra* note 42.

⁹² Linkous, *supra* note 29 at 10.

sued, but if they fail to do so this immunity vanishes.⁹³ there is an exception for copyright claims, leaving websites vulnerable lawsuits for the republishing of victim’s copyrighted images.⁹⁴ In terms of effective remedies addressed thus far, DMCA takedowns and copyright claims brought by victims of revenge porn seems to actually effect the heart of the matter, which is removing the intimate images.

Many websites have responded positively to these takedown notices. For example, the popular website, Reddit, took down images after receiving threats of copyright suits by victims.⁹⁵ Reddit did not take down the images because of an overwhelming feeling of sympathy for the victims; it did so because it faced legal consequences.⁹⁶ Copyright law is the first law to actually make the revenge porn images the problem of the host website.⁹⁷ Like with all things good, there is always bad. After receiving copyright notices for his website isanyoneup.com, Hunter Moore took the less civil approach by ignoring the notices and publicizing the images more in retaliation.⁹⁸ Overall, victims initiating DMCA takedown procedures has proved to be “the path of least resistance.”⁹⁹

As with all of the previously discuss remedies, copyright law also has major drawbacks to its ultimate effectiveness. First, copyright law does not have the same deterrent effect on future revenge porn postings as does criminal law.¹⁰⁰ The continued increase in websites dedicated to revenge porn and the increase in revenge porn uploads supports this belief regarding deterrence.¹⁰¹

⁹³ Fiedler, *supra* note 29 at 188-89.

⁹⁴ Linkous, *supra* note 29 at 11.

⁹⁵ Dewey, *supra* note 85.

⁹⁶ *Id.*

⁹⁷ *Id.*

⁹⁸ *Id.*

⁹⁹ *Id.*

¹⁰⁰ Linkous, *supra* note 29 at *11.

¹⁰¹ Cyber Civil Rights Initiative, *supra* note 30.

Second, once a image is posted it generally spreads across the internet like a wildfire.¹⁰² A victim may be able to get the images taken down from one site, but there may be numerous other locations where the images remain on the Internet.¹⁰³ Third, in order to actually send out a take-down notice the victim must register the images with the US Copyright Office.¹⁰⁴ The registration process requires the victim to use his or her own name, bringing more attention to the problem that the victim is trying to hide.¹⁰⁵ Finally, if the victims affected did not take the image themselves, they cannot bring a copyright claim because they are not the owner of the image.¹⁰⁶

Consistent with all legal remedies currently available in the US, copyright law has its benefits and detriments. Unlike the above mentioned causes of action, however, copyright law is the only one that does what victims want: it get[s] their misappropriated imaged off the Internet.”¹⁰⁷

III. The Right to Be Forgotten

A. Emergence of the Right to Be Forgotten

In 2014, the European Union Court of Justice (“CJEU”) announced a decision in *Google Spain* that would alter the general immunities given to website operators.¹⁰⁸ The CJEU announced the rule,

An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties. Thus, if, following a search made on the basis of a person’s name, the list of results displays a link to a web page which contains information on the person in question, that data

¹⁰² Linkous, *supra* note 29 at *11.

¹⁰³ Citron, *supra* note 40 at 122.

¹⁰⁴ Alex Ronan, *Could All These New Revenge-Porn Laws Actually Be a Bad Thing?*, New York Magazine (Apr. 16, 2015, 9:20AM), <http://nymag.com/thecut/2015/04/why-regulating-revenge-porn-is-so-tricky.html#>.

¹⁰⁵ Goldnick, *supra* note 36 at 611.

¹⁰⁶ Cyber Civil Rights Initiative, *supra* note 30.

¹⁰⁷ Dewey, *supra* note 85.

¹⁰⁸ See Generally Jeffrey Toobin, *The Solace of Oblivion: In Europe, the Right to Be Forgotten Trumps the Internet*, The New Yorker (Sep. 29, 2014), <http://www.newyorker.com/magazine/2014/09/29/solace-oblivion#> (“All individuals in the countries within its jurisdiction had the right to prohibit Google from linking to items that were “inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed”).

subject may approach the operator directly and, where the operator does not grant his request, bring the matter before the competent authorities in order to obtain, under certain conditions, the removal of that link from the list of results.¹⁰⁹ The conditions necessary for removal are that the information linked to must be: (1) inaccurate, (2) inadequate, (3) irrelevant, or (4) excessive.¹¹⁰

The *Google Spain* case began when a Spanish citizen, Mario Costeja Gonzalez, ran into debt and his property was headed for auction.¹¹¹ The newspaper *La Vanguardia* reported on the auction and the article remained linked on the Internet despite Costeja clearing up his debts and avoiding the property auction.¹¹² Costeja brought suit against Google Spain claiming the information linked in Google's search results "infringed his privacy rights because the proceedings concerning him had been fully resolved for a number of years and hence the reference was entirely irrelevant."¹¹³ The CJEU found that under the 1995 Data Protection Directive, there existed a Right to Be Forgotten.¹¹⁴ Article 12 defines the Right of Access as follows,

Member States shall guarantee every data subject the right to obtain from the controller: [...] (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data; (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.¹¹⁵

¹⁰⁹ Press Release No 70/14, E.C.J. (May 13, 2014), available at <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf>.

¹¹⁰ European Commission, *Factsheet on the "Right to Be Forgotten" Ruling*, available at http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

¹¹¹ Toobin, *supra* note 106.

¹¹² *Id.*

¹¹³ European Commission, *supra* note 108.

¹¹⁴ *Id.*

¹¹⁵ Eur. Parl. Doc. (COM 31995L0046) 1995, available at <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en>.

While an entirely new rule was not created, the CJEU did interpret Article 12 in a revolutionary and broad-reaching way, as had never been seen before in cases regarding the internet and privacy.¹¹⁶

In practice, the ruling in *Google Spain* has impacted information on the internet severely.¹¹⁷ In the span of less than a year, Google has received approximately one hundred and twenty thousand requests for deleting information, although Google has only granted about half of them.¹¹⁸ Google is now caught in the middle of a Privacy versus Internet debate. Google has nothing to do with posts online, all the service does is index them to make searching for these materials simpler.¹¹⁹ In the EU, Google is responsible for making sure the Internet does not remember forever.¹²⁰ The EU is using the Right to Be Forgotten almost as a replacement for the natural effects of time.¹²¹ Time used to take care of “forgetting” news, as newspapers would fade or rot and photographs would be misplaced or lost.¹²²

To implement the CJEU ruling, Google needed to do carry out two procedures: (1) create a software infrastructure to be used to remove the links and (2) create an administrative system for sorting through removal requests.¹²³ The removal request forms, similar to copyright claims, requires an individual’s name and the links which he or she takes issue with.¹²⁴ In an attempt to please both private citizens and website operators, Google notifies the website that hosts the link

¹¹⁶ European Commission, *supra* note 108.

¹¹⁷ Toobin, *supra* note 106.

¹¹⁸ *Id.*

¹¹⁹ Matt Rosoff, *This Ruling Shows the Absurdity of Europe’s ‘Right to Be Forgotten’ Law*, Business Insider (Aug. 20, 2015, 2:04PM), <http://www.businessinsider.com/eu-right-to-be-forgotten-law-is-idiotic-2015-8>.

¹²⁰ *Id.*

¹²¹ See Generally Lawrence Shy, Article, *Forget Me, Forget Me Not: Reconciling Two Different Paradigms of the Right to Be Forgotten*, 103 Ky. L. J. 311, 313 (2014).

¹²² *Id.*

¹²³ Toobin, *supra* note 106.

¹²⁴ *Id.*

in question and gives the operators a chance to explain why a link should be kept.¹²⁵ The website generally responds, which leads Google to carry out a balancing test. This test involves “whether the individual is a public or a private figure; whether the link comes from a reputable news source or government Web site; whether it was the individual who originally published the information; and whether the information relates to political speech or criminal charges.”¹²⁶

Google has tended to grant private citizens’ requests more often than public officials, but with the sole discretion granted to the search engine theoretically anyone can have anything taken down.¹²⁷

While many EU citizens praise the decision by the CJEU, an equal amount find the ruling preposterous and dangerous. For example, Google has recently received orders to take down links to current news stories because they involve the same person who submitted removal requests for older links.¹²⁸ The removal orders are “akin to asking libraries to remove news stories about individuals from their archives.”¹²⁹ Other critics cite the desire for individuals to only have “correct” or positive information on the Internet as a reason why the Right to Be Forgotten should not exist.¹³⁰ Some even believe the Right to Be Forgotten is inherently anti-Internet.¹³¹ The Internet, although seemingly interminable, has a natural process of degradation where links and files are slowly lost or changed as websites disappear over time.¹³² Whether or not the Right to Be

¹²⁵

Id.

¹²⁶

Id.

¹²⁷

Id.

¹²⁸

Matt Rosoff, *supra* note 117.

¹²⁹

Id.

¹³⁰

See Generally Daniel Fisher, *Europe’s ‘Right to Be Forgotten’ Clashes with U.S. Right to Know*, FORBES (May 16, 2014, 8:45AM), <http://www.forbes.com/sites/danielfisher/2014/05/16/europes-right-to-be-forgotten-clashes-with-u-s-right-to-know/>.

¹³¹

Shy, *supra* note 119 at 339.

¹³²

Id. at 340 (“Internet information is particularly susceptible to degradation, primarily from technical conditions that require individual sites to be maintained as time passes. Additionally, as sites are preserved and updated, information that might be the target of an asserted ‘Right to Be Forgotten’ is lost as individual pages are changed”).

Forgotten too much favors the right of Privacy will be an ongoing debate; but for the time being, the implications of being able have a “clean slate” is formidable.¹³³

B. European Ideals of a Right to Privacy

Underpinning much of the ruling in *Google Spain* is a general interest in the right of Privacy possessed by all individuals in the EU.¹³⁴ The European Convention on Human Rights expressly grants all citizens a right to Privacy that States cannot interfere with.¹³⁵ Behind these laws lies strong dignitary traditions, where there is a presumption of legal relief when an individual believes their honor or dignity has been scandalized.¹³⁶ The decision in *Google Spain* was a victory for privacy across the European Union.¹³⁷

V. Bringing the Right to Be Forgotten to the US

A. The Constitutional Roadblock

The US Constitution First Amendment provides, “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.”¹³⁸ The US does not possess a “right of Privacy” comparable to the EU, with only a few categories of sensitive information receiving protection.¹³⁹

¹³³ Lindsay Hoffman, *Do We Have a Right to Be Forgotten?*, Huffington Post (Jul. 16, 2015, 2:55PM), http://www.huffingtonpost.com/lindsay-hoffman/do-we-have-a-right-to-be_b_7812564.html.

¹³⁴ *Id.*

¹³⁵ *Id.*

¹³⁶ Lisa Fleisher, *Google Ruling: Freedom of Speech vs. the Right to Be Forgotten*, Wall Street Journal (May 23, 2014, 2:10PM), <http://blogs.wsj.com/digits/2014/05/13/eu-court-google-decision-freedom-of-speech-vs-right-to-be-forgotten/>.

¹³⁷ *Id.*

¹³⁸ U.S. Const. amend. I

¹³⁹ Toobin, *supra* note 73 (“When it comes to privacy, the United States’ approach has been to provide protection for certain categories of information that are deemed sensitive and then impose some obligation not to disclose unless certain conditions are met. Congress has passed laws prohibiting the disclosure of medical information (the Health Insurance Portability and Accountability Act), educational records (the Buckley Amendment), and video-store rentals (a law passed in response to revelations about Robert Bork’s rentals when he was nominated to the Supreme Court)).

The right to free speech is so strong in the US that the *Google Spain* decision would not have occurred.¹⁴⁰ The case could not have been decided in favor of the plaintiff because “the records were public, and they were reported correctly by the newspaper at the time; constitutionally, the press has a nearly absolute right to publish accurate, lawful information.”¹⁴¹

To combat unprotected speech, the US generally relies on tort law to protect citizens from libel, defamation, and invasion of privacy.¹⁴² Additionally, Congress implemented the CDA for the very purpose of allowing the Internet to expand to its fullest potential.¹⁴³ The Internet is the ultimate forum for free speech, with individuals exchanging ideas, images, expressions, etc. on a rapid basis with almost no obstruction.¹⁴⁴ What makes the US’s position in the revenge porn phenomenon so unique is the interplay of tort law, the First Amendment, and the CDA. Uploading revenge porn may not be protected speech since reputation of private citizens “trumps” protection, which allows tort law remedies.¹⁴⁵ But these tort law remedies do not remove the information from the internet, since the Internet (in particular website operators) enjoy immunity from claims against third-parties under the CDA. Since the current ways to bring claims against unprotected speech under the First Amendment do not actually redress the harms felt by victims of revenge porn, a new approach is needed within the US that both helps victims and stays within the bounds of the Constitution. This is where a modified Right to Be Forgotten law would fit perfectly.

In *Hustler Magazine v. Falwell*, the United States Supreme Court addressed a claim of Intentional Infliction of Emotional Distress as a way around First amendment protections given to

¹⁴⁰

Id.

¹⁴¹

Id.

¹⁴²

Fisher, *supra* note 128.

¹⁴³

Goldnick, *supra* note 36 at 600.

¹⁴⁴

Larkin, *supra* note 38 at 97.

¹⁴⁵

Geoffrey R. Stone, *Privacy, the First Amendment, and the Internet*, in *The Offensive Internet: Speech, Privacy, and Reputation* 174, 175 (Saul Levmore & Martha C. Nussbaum eds., 2010).

the public realm.¹⁴⁶ A minister brought suit against *Hustler Magazine* for a parody it published involving the minister.¹⁴⁷ The Supreme Court ultimately held, “public figures and public officials may not recover for the tort of intentional infliction of emotional distress” unless it can be shown actual malice the publication used actual malice.¹⁴⁸ *Hustler Magazine* is illustrative of the cases where the Supreme Court rules in favor of free speech. Public discourse is essential to the nation’s values, and speech cannot be limited when it involves public figures.¹⁴⁹ The case does not involve private citizens, which leaves open even the smallest of cracks for a discussion on how to handle cases of nonconsensual pornography. The decision in *Hustler Magazine* is as significant for what it holds, as for what it does not. It does not preclude private citizens from claiming Intentional Infliction of Emotional Distress against the First Amendment. The Supreme Court did not preclude ruling on the “outrageousness” of content in private settings either, perhaps leaving room for an edited version of the Right to Be Forgotten.

B. Transmuting the Right to Be Forgotten to Redress Victims of Revenge Porn

In its current state, the Right to Be Forgotten would not conform with the US Constitution. The right of free speech goes hand-in-hand with the freedom of the press and a quasi-right to be remembered.¹⁵⁰ The collection and publication of information, for both public officials and private citizens, is a cornerstone to the free-flow of ideas in the US.¹⁵¹ Since the US has such a pervasive and broad notion of the right to free speech, allowing private citizens *and* public officials to send in request forms to have information delinked on websites would be extreme. If narrowly tailored,

¹⁴⁶ *Hustler Magazine v. Falwell*, 485 U.S. 46, 48 (1988).

¹⁴⁷ *Id.*

¹⁴⁸ *Id.* at 56.

¹⁴⁹ *See generally* Stone, *supra* note 143 at 188.

¹⁵⁰ *See generally* Shy, *supra* note 119 at 331.

¹⁵¹ *Id.*

however, the Right to Be Forgotten could play a major role in providing a uniform remedy for redressing victims of revenge porn.

The power of having a Right to Be Forgotten law in the US stems from how the Internet ultimately works. Most, if not all, of the internet's users go through search engines, unless they know exactly what they are looking for.¹⁵² If victims can submit a form to have search engines delink to the images, "it becomes like a tree falling in the forest. There may be links out there, but if you can't find them through a search engine they might as well not exist."¹⁵³ When items are delinked by Google, for example, it becomes increasingly harder for them to be found or spread around the web.

With the current system implemented by the E.U., it would not be difficult for US search engines to modify forms to only include removal requests for revenge porn. A difficult aspect would be the need to use given names (no anonymous claims) and the inclusion of the links to be removed, but ultimately the process provides victims with the swiftest, most cost-effective remedy. Limited requests to revenge porn would not conflict with the US's notions of free speech, because private information and news stories are not protected the same as public reports.¹⁵⁴ Some proponents of a global Right to Be Forgotten cite to the use of removal proceedings by Google to when copyright claims are filed.¹⁵⁵ Links are removed immediately when takedown notices are filed, which means the technical removal software is already in place; all that would need to be amended is the administrative system to include revenge porn claims.¹⁵⁶

¹⁵² Toobin, *supra* note 106.

¹⁵³ *Id.*

¹⁵⁴ Farhad Manjoo, 'Right to Be Forgotten' Online Could Spread, *The New York Times* (Aug. 5, 2015), http://www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html?_r=0.

¹⁵⁵ *Id.*

¹⁵⁶ *Id.*

Creating a federal Right to Be Forgotten law would also just be a reflection of the trend already occurring within the US. In June, Google altered its own site nudity policies to include removal of revenge porn.¹⁵⁷ Historically, Google’s resistance towards erasing data made it the supreme search engine as it processes nearly two-thirds of all information requests online.¹⁵⁸ Amit Singhal, a Senior Vice President for Google, stated “our philosophy has always been that Search should reflect the whole web. But revenge porn images are intensely personal and emotionally damaging, and serve only to degrade the victims—predominantly women.”¹⁵⁹ Google’s new policy allows revenge porn takedown requests to be filtered with copyright claims and other removal requests for personal information.¹⁶⁰

Similarly, Microsoft announced new procedures for removing links to revenge porn images from its search engine results.¹⁶¹ Jacqueline Beauchere, Microsoft’s Chief Online Safety Officer, detailed, “Microsoft will remove links to photos and videos from search results in Bing, and remove access to the content itself when shared on OneDrive or Xbox Live, when we are notified by a victim.”¹⁶² Major search engine sites have taken their own actions to combat revenge porn, so why not make it a national policy across the board for website operators?

A surge of individual Right to Be Forgotten policies targeted to revenge porn uploads have occurred in the US over the past year. If the US were to implement a Right to Be Forgotten policy for all search engines, it would only continue this trend to remedy the embarrassing and heinous

¹⁵⁷ Associated Press, *Google Cracks Down on ‘Revenge Porn’ Under New Nudity Policy*, The Daily Mail (Jun. 19, 2015, 5:19PM), <http://www.dailymail.co.uk/sciencetech/article-3131990/Google-cracks-revenge-porn-new-nudity-policy.html>.

¹⁵⁸ *Id.*

¹⁵⁹ Amit Singhal, *‘Revenge Porn’ and Search*, Public Policy Blog (Jun. 19, 2015), <http://googlepublicpolicy.blogspot.com/2015/06/revenge-porn-and-search.html>.

¹⁶⁰ *Id.*

¹⁶¹ Jacqueline Beauchere, *‘Revenge porn:’ Putting Victims Back in Control*, Public Policy Blog (Jun. 22, 2015), <http://blogs.microsoft.com/on-the-issues/2015/07/22/revenge-porn-putting-victims-back-in-control/>.

¹⁶² *Id.*

acts of revenge porn. A targeted and extremely limited variant on the Right to Be Forgotten would in essence do what congress always intended: to have internet service providers self-regulate the content published within its online space. While creating a law seems counter-intuitive to self-regulation, website operators as a whole have not stepped up until very recently to even contemplate self-regulation. Once the decision in *Zeran* came down after the passing of the CDA, internet service providers shirked their end of the bargain. Establishing a federal law where website operators would need to provide *at a minimum* a submission form for delinking to websites or articles solely based on claims of nonconsensual pornography would neither violate the First Amendment, nor would it run counter to congressional intent behind §230.

Ultimately, having an out-of-court remedy where victims can request to have nonconsensual pornographic images either removed or delinked by internet service providers is a simple solution to a vicious and all too common problem. Victims would not have to feel helpless if they did not take the image themselves or defeated if the perpetrator did not act criminally or if the perpetrator does not have deep enough pockets to even cover the cost of litigating a claim. The Right to Be Forgotten, in an extremely tailored form, would provide victims with a path of least resistance to the fundamental aim: to minimize the harm done by reducing the number of individuals who see the nonconsensual pornographic post.

V. Conclusion

The protections given to website operators under §230 of the CDA “promotes a culture of irresponsibility when it comes to speech online.”¹⁶³ The consistent granting of immunity by US courts have forced victims of nonconsensual pornography to seek alternate paths for redress. Some opt for the costly civil suit against the defendant’s themselves, which only yields as much success

¹⁶³ David J. Solove, *Speech, Privacy, and Reputations on the Internet*, in *The Offensive Internet: Speech, Privacy, and Reputation* 15, 23 (Saul Levmore & Martha C. Nussbaum eds., 2010).

as the individual is financially worth. Some victims choose the criminal path, which is less costly but has higher standards for finding guilt. Finally, some have resorted to copyright law and DMCA takedown notices, where only victims who took a “selfie” can pay the price to save their dignity.

Revenge porn continues to be an issue within the US because it implicates so many variations of existing laws, while no one law covers revenge porn as an all-encompassing crime. The current laws within the US do not work as a holistic solution since,

Every case of revenge porn is different: some photos are selfies and some aren't; some were hacked and some were uploaded by exes; some victims are under 18, and some are well over it. Different laws and legal concepts apply in each of those cases, which makes any kind of comprehensive approach impossible.¹⁶⁴

Copyright claims only apply to a small fragment of victims who can show they took the image themselves and therefore possess a copyright.¹⁶⁵ This closes off any victim who was hacked, unknowingly recorded, or knowingly recorded from pursuing this claim. Tort actions where victims claim IIED, harassment, or defamation must meet certain standards when accusing perpetrators of such actions.¹⁶⁶ Additionally, these suits can be extremely expensive and time-consuming, thus precluding another section of victims who cannot pursue this recourse. Finally, criminal laws are not adopted by every state and meeting criminal standards can be extremely difficult for victims when a perpetrator has uploaded one nonconsensual image, one time, to one website.¹⁶⁷

The Right to Be Forgotten, at least in a modified in narrowly tailored form, aids to fill the gaps between each area of existing legal coverage. In cases where an image is taken by another and posted without defamatory information attached, there is no remedy for the victim where the

¹⁶⁴ Dewey, *supra* note 85.

¹⁶⁵ Cyber Civil Rights Initiative, *supra* note 30.

¹⁶⁶ *Id.*

¹⁶⁷ Cyber Civil Rights Initiative, *supra* note 62.

image is removed from the Internet. While the Right to Be Forgotten does not remove individual images, simply delinking from websites that house nonconsensual pornography is a much needed step towards concealment for the victims. A variant on the Right to Be Forgotten would be a gap-filler for all of the cases not covered by current US laws. Victims could go right to the internet service provider to have content delinked before deciding whether or not to pursue a claim in court. Criminal punishment, tort laws, and copyright claims all do their individual part to aid victims of revenge porn, but the Right to Be Forgotten would help all victims no matter the factual nuances surrounding the uploaded images.