Northwest Missouri State University

From the SelectedWorks of Allison L Tungate

March 24, 2014

Bare Necessities: The Argument for a “Revenge Porn” Exception in Section 230 Immunity

Allison L Tungate

Available at: https://works.bepress.com/allison_tungate/1/
Bare Necessities: The Argument for a “Revenge Porn” Exception in Section 230 Immunity

Internet Law
Allison Tungate
I. INTRODUCTION

Within the past few years, “sexting” has become an intricate part in American language and culture, influencing both teens and young adults. Merriam Webster Online Dictionary defines sexting as, “the sending of sexually explicit messages or images by cell phone.” According to a 2008 survey of 653 teens and 627 young adults by The National Campaign to Prevent Teen and Unplanned Pregnancy, 20% of teens and 33% of young adults overall sent or posted online nude or semi-nude pictures or videos of themselves. Many teens and young adults see nothing wrong with sexting and view such conduct as another way to flirt, cultivate relationships, or express their sexuality.

However, sexting as a commonplace activity in 21st century relationships is creating adverse consequences when such photos and videos are shared with those other than the intended recipient. Specifically, web operators are capitalizing on the concept of “revenge porn.” Revenge porn, also known as “involuntary pornography,” is the online posting of nude or sexual photographs of a former lover without his or her consent.

Other methods of acquiring such photographs are through hacking, theft by repair people

---

2 I will define “teens” as those between the ages of 13-19 as set forth by The National Campaign to Prevent Teen and Unplanned Pregnancy. See Sex and Tech: Results From a Survey of Teens and Young Adults, http://www.thenationalcampaign.org/sextech/PDF/SexTech_Summary.pdf.
3 I will define “young adult” as those between the ages of 20-26 as set forth by The National Campaign to Prevent Teen and Unplanned Pregnancy. See Sex and Tech: Results From a Survey of Teens and Young Adults, http://www.thenationalcampaign.org/sextech/PDF/SexTech_Summary.pdf.
5 Supra notes 1 & 2.
7 Lorelei Laird, Striking Back at Revenge Porn Victims Are Taking on Websites for Posting Photos They Didn’t Consent to, ABA J., November 2013, at 44, 46.
and false personal ads. As a result, websites such as MyEx.com, create a forum for scorned ex-lovers, embittered friends, and malicious hackers to submit and share semi-nude and nude photographs. Revenge porn websites exist to seek revenge on former paramours by instigating a form of psychological warfare. Because content is “generally posted with the subject’s real name, city and state, and often links to social media profiles,” the “revenge factor” is real and often adversely affects a victim’s ability to get or maintain a job. Additionally, many victims and their families are threatened with violence.

Because of the shock-factor of revenge porn, the question of the legality of websites featuring such content is raised. The answer lies in Section 230 of the Federal Communications Decency Act (“Section 230”), also known as the “Good Samaritan” provisions. In short, Section 230 provides protection for website operators and providers of an “interactive computer service” from information posted by a third party. Hunter Moore, founder and creator of the revenge porn website “IsAnyoneUp?,” was quoted in a 2011 interview with Forbes Magazine, saying, “It (the Act) kind of sucks…well, if I wasn’t in this whole game.” Indeed, Section 230 creates a safe harbor

---

8 Id.
10 Laird, Striking Back at Revenge Porn Victims Are Taking on Websites for Posting Photos They Didn’t Consent to, at 46.
11 Id.
from liability for web operators like Moore who host a forum for malicious and defamatory\textsuperscript{16} content, which in turn “sucks” for victims of revenge porn.

In this article, I will first analyze the legal impact of Section 230 for web operators, Internet service providers (“ISPs”), and victims of revenge porn. I will focus on existing case law pertaining to Section 230 and the overall detrimental effect the holdings have created for victims of revenge porn. I will then discuss potential routes both in the realm of civil and criminal law that victims may pursue in order to seek a remedy and/or compensation—specifically against website providers and the posters of the unauthorized content. For each route, I will highlight the obstacles victims of revenge porn face for each claim, which in turn will demonstrate the inadequacy of pursuing such claims. I will then discuss recently passed laws in New Jersey and California aimed at combating revenge porn and highlight the advantages and disadvantages of each law.

Last, I will discuss the merits of changing Section 230 in such a way as to provide a legal remedy for victims of revenge porn. Specifically, I will propose an exception to the safe harbor of Section 230 that establishes a takedown procedure. The takedown requirement of the exception, narrowly-tailored to apply only to websites featuring revenge porn content, will allow victims to pursue a more feasible remedy, rather than those provided by state criminal and civil actions. I will then identify “freedom of expression” concerns regarding the proposed exception and explain why revenge porn is unprotected by the First Amendment.

\textsuperscript{16} “Defamatory” in the sense of damaging the good reputation of someone.
II. LEGAL IMPACT OF THE SECTION 230 SAFE HARBOR OF THE COMMUNICATION DECENCY ACT

A. Background

In 1995, a New York state court characterized an interactive computer service as a publisher, and accordingly, held such services were liable for defamatory content made by users on its virtual bulletin boards.\(^\text{17}\) With the advent of the Internet creating a whole new world of free speech and the possibility of a wave of tort-based lawsuits causing a “chilling effect” of such speech,\(^\text{18}\) Congress enacted the Communication Decency Act (“CDA”) in order to “carve out a sphere of immunity from liability” for those who provide interactive computer services. Namely, the goal of the CDA is the preservation of a “vibrant and competitive free market” of ideas on the Web.\(^\text{19}\) Congress also used the CDA as a response to rising concerns of Internet pornography and potential strict liability for ISPs who posted defamatory content on their websites.\(^\text{20}\) In order to achieve a “vibrant and competitive free market” of ideas, Congress enacted Section 230 of the CDA, which unambiguously provides blanket immunity for websites and other services that allow user-generated content.\(^\text{21}\) Congress established that Section 230 allows ISPs to self-regulate content without concern of being liable for defamatory content that is either overlooked or chosen to remain on the site.\(^\text{22}\)


\(^{19}\) 52 A.L.R. Fed. 2d 37 (Originally published in 2011).


\(^{22}\) See Medencia, The Immutable Tort of Cyber-Defamation, supra note 14 at 4.
B. Zeran v. American Online, Inc.

As a result, Section 230 provides liability immunity for website providers and their services from any claims stemming from content posted by third parties.\textsuperscript{23} Courts have continuously reinforced this notion.\textsuperscript{24} As stated in \textit{Zeran v. American Online, Inc.}, the U.S. Court of Appeals for the Fourth Circuit reasoned:

\begin{quote}
It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and types of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.\textsuperscript{25}
\end{quote}

After its passing in 1996, \textit{Zeran} was one of the first cases to test the strength of Section 230.\textsuperscript{26} The dispute in \textit{Zeran} involved a prank that occurred a few days after the Oklahoma City bombing when an anonymous AOL subscriber posted Kenneth Zeran’s personal information on an advertisement for a highly offensive T-shirt praising Timothy McVeigh’s terrorist attack.\textsuperscript{27} After being notified of the prank, Zeran was subjected to a wave of threatening and harassing phone calls.\textsuperscript{28} Because Zeran could not change his phone number since his business relied on its availability to the public, he contacted AOL

\begin{footnotes}
\textsuperscript{23} \textit{Id.}


\textsuperscript{25} See Fenn, Humphries, \textit{Protection Under CDA § 230 and Responsibility for "Development" of Third-Party Content, supra} note 17 at 28 (quoting \textit{Zeran}, 129 F.3d at 331).

\textsuperscript{26} See Medencia, \textit{The Immutable Tort of Cyber-Defamation, supra} note 14 at 5.

\textsuperscript{27} \textit{Id.}

\textsuperscript{28} \textit{Zeran v. Am. Online, Inc.}, 129 F.3d 327, 329 (4th Cir. 1997).
\end{footnotes}
asking them to remove the posting. Additional messages similar in nature were posted purporting to be Zeran selling items with offensive slogans in relation to the Oklahoma City bombings and Timothy McVeigh. As a result, Zeran sought to hold AOL liable for defamatory speech initiated by a third party. He alleged that once he notified AOL of the hoax, they “had a duty to remove the defamatory posting promptly, to notify the subscribers of the message’s false nature, and to effectively screen future defamatory material.” The court dismissed all three arguments.

Rejecting Zeran’s argument, the court noted that Congress made the policy choice of not holding companies serving third parties liable for potentially injurious messages. Instead, the court reinforced the idea that only the original party who posted the defamatory message would be culpable and thus held accountable. Additionally, the court held that AOL was a publisher and hence “clearly protected by Section 230’s immunity,” based on Congress’s intent. Thus, the CDA bars lawsuits seeking to hold ISPs liable for functioning like a traditional publisher with regards to editing and deciding whether to publish, withdraw, postpone or alter content.

Consequently, the holding in Zeran has reinforced the safe harbor set forth by Section 230. Zeran established the significant notion that even if victims put the ISPs or web operators on notice about defamatory photos or videos, no duty exists requiring such

---

29 Zeran, 129 F.3d at 329.
30 Id. at 329.
31 Id. at 330.
32 Id.
33 Id.
34 Zeran, 129 F.3d at 331-32.
35 Id. at 330.
36 Id. at 331.
37 Id. at 330.
service providers to remove the offensive content. Thus, culpability exists only in the
poster of the defamatory content and ISPs and web operators are within the safe harbors
of Section 230.\(^{38}\) Despite \textit{Zeran} being decided over sixteen years ago, the Section 230
safe harbor has been consistently broadly construed and protected under the law.\(^{39}\)

\textbf{C. Section 230 and Federal and State Common Law}

In \textit{Zeran}, the Fourth Circuit articulated quite clearly the implications of Section
230 on state law: “While Congress allowed for the enforcement of ‘any State law that is
consistent with [§ 230],’ it is equally plain that Congress’ desire to promote unfettered
speech on the Internet must supersede conflicting common law causes of action.”\(^{40}\)
Specifically, Section 230 preempts any state laws to the contrary: ",[n]o cause of action
may be brought and no liability may be imposed under any State or local law that is
inconsistent with this section."\(^{41}\)

Notably, the significance of this preemption is found in distinguishing the
definitions of “publisher” between state and federal law. Section 230 articulates ",[n]o
provider or user of an interactive computer service shall be treated as the publisher or
speaker of any information provided by another information content provider."\(^{42}\)
Traditionally, “publishers” were information providers such as newspapers, magazines or
television and radio stations who would be held liable for any defamatory content

\(^{38}\) \textit{See supra} note 29.
immunity from defamation claim; court determined Congress made policy choice in “providing immunity
even where the interactive service provider has an active, even aggressive role in making available content
prepared by others.”); \textit{Green v. AOL}, 318 F.3d 465 (3rd Cir. 2003) (holding Section 230 safe harbor
provided AOL with immunity from negligence claim stemming from allegation AOL failed to adequately
police its services, causing plaintiff to be defamed and inflicted with intentional emotion distress by third
parties).
\(^{40}\) \textit{Zeran}, 129 F.3d 327, 334 (4th Cir. 1997).
\(^{42}\) 47 U.S.C.A. § 230(c)(1) (West).
published or distributed over their respective mediums.\textsuperscript{43} However, Congress made the explicit policy decision to exclude ISPs from being considered as “publishers” under the traditional common law sense.\textsuperscript{44} Consequently, because of Congress’ policy choice to differentiate ISPs from traditional information providers, victims of revenge porn cannot turn to state common law that is inconsistent with Section 230 for relief.

Alternatively, Section 230 has no effect on federal criminal law or intellectual property law.\textsuperscript{45} In relation to Section 230(e)(1), courts have “considered whether its limitation on the construction of Section 230(c) to impair the enforcement of federal criminal law applied to limit immunity for civil claims.”\textsuperscript{46} Despite possible limitations on civil claims stemming from federal criminal law violations, victims may be able to find relief in copyright law, since intellectual property claims are an exception to Section 230 preemption.\textsuperscript{47} Section 230 explicitly states that it is the policy of the United States to “ensure vigorous enforcement of [f]ederal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.”\textsuperscript{48} Although preempting

\begin{itemize}
\item \textsuperscript{43} \textit{Batzel v. Smith}, 333 F.3d 1018, 1026-27 (9th Cir. 2003).
\item \textsuperscript{44} Id. at 1027 (describing the various policy reasons for treating ISPs differently than traditional information providers).
\item \textsuperscript{45} 47 U.S.C.A. §§ 230(e)(1)-(2) (West).
\item \textsuperscript{46} 52 A.L.R. Fed. 2d 37 (Originally published in 2011); \textit{See Noah v. AOL Time Warner, Inc.}, 261 F. Supp. 2d 523 (E.D. Va. 2003), summarily aff’d, 2004 WL 602711 (4th Cir. 2004) (declining to find that the exception to immunity applicable to federal criminal statutes of Section 230(e)(1) applied to claims brought under a federal civil rights statute); \textit{Doe v. Bates}, 35 Media L. Rep. (BNA) 1425, 2006 WL 3813758 (E.D. Tex. 2006) (unreported opinion) (granting a motion to dismiss a civil claim based upon violations of federal child pornography law because the claim did not fall within the limitations to the immunity granted by the CDA for enforcement of federal criminal statutes); \textit{Dart v. Craigslist, Inc.}, 665 F. Supp. 3d 961 (N.D. Ill. 2009) (determining that 18 U.S.C.A. 1952, making it unlawful to use any facility in interstate commerce with the intent to “promote” or “facilitate the promotion” of any unlawful activity, including prostitution offenses, did not bring a public nuisance suit within the limitation for federal criminal law found in Section 230(e)(1)).
\item \textsuperscript{47} \textit{See infra} notes 53-64.
\item \textsuperscript{48} 47 U.S.C.A. § 230(b)(5).
\end{itemize}
state criminal law, Section 230(e)(1) allows the government to allege federal criminal violations against ISPs that would otherwise be shielded from liability. 49

III. POTENTIAL REMEDIES FOR REVENGE PORN VICTIMS

Because revenge porn is increasing in popularity, victims have turned to the legal system for relief. However, due to the widespread effects of liability established by Section 230 of the CDA, many of these remedies are ineffective and present massive hurdles and challenges for victims. The following sections discuss potential remedies and their effectiveness for revenge porn victims seeking relief.

A. Civil Suit Cause of Action: Invasion of Privacy

As established in Zeran, the court rejected the retention of common law principles that would hold distributors of malicious and defamatory content liable, and instead upheld Congress’s usage of “publisher” to mean both distributors and original publishers. 50 However, victims of revenge porn can potentially find solace in common law actions of invasion of privacy. It is important to note, though, that this cause of action focuses on the perpetrator posting the defamatory content, not the ISP.

With regards to an invasion of privacy action, which protects the “right to be left alone,” 51 the Restatements (Second) of Torts identifies four different privacy torts that encompass the right to privacy: “(1) intrusion upon a plaintiff’s seclusion or solitude, (2) appropriation of the plaintiff’s name or likeness, (3) public disclosure or embarrassing of a plaintiff’s private facts, and (4) publicity placing plaintiff in false light in the public

50 Zeran, 129 F.3d at 334.
Early in the emergence of the invasion of privacy action, there was growing concern that “recent inventions and business methods” in technology would lead to threats against the right to privacy. Despite an initial application to only physical intrusions, courts today have been willing to apply the intrusion tort to cases involving harassing phone calls, spying on others in bathrooms, and circulating nude photographs after being dropped off at a business for developing.

Accordingly, victims of revenge porn can bring forth a common law claim of invasion of privacy, since the right protects against “any type of prying or intrusion into anything the plaintiff would consider private.” The Restatement (Second) of Torts outlines the four prongs to an invasion of privacy claim: “(1) Public disclosure; (2) of a private fact; (3) which would be offensive and objectionable to the reasonable person; and (4) which is not of legitimate public concern.” Thus, a victim of revenge porn would have to make his or her case that a private photo or video not of public concern was made public, and a reasonable person would object to such public disclosure. A victim would likely succeed on an invasion of privacy claim because he or she would make an argument that a nude photograph or video depicting sexual activity is not a legitimate public concern and is patently offensive and objectionable to the reasonable person.

---

53 Id. at 172; (Lawyer Samuel D. Warren and future Supreme Court Justice Brandeis actively voiced this concern).
However, a victim’s success in an invasion of privacy claim does not necessarily translate into the picture being taken down by the website, as the lawsuit would only affect the poster because of the Section 230 safe harbor. Also problematic for victims is that the poster loses control of the content once it is submitted to a website. Regardless of the outcome of the invasion of privacy claim, the website operator has no obligation or duty to take down the content at issue. Additionally, once a photograph is posted on the Internet and shared among users, it is very costly and time consuming to completely eradicate the photo from the Internet or a Google search.\footnote{If offensive content is posted, an individual can contact the website and request its removal. If the website does not comply and the individual took the photo his or herself, then he or she could be eligible for a DMCA takedown request. There is a high possibility that the content has been shared and copied, so the onus will be on the individual to contact and submit a takedown request for each website the content appears. Additionally, the individual can request a court order to get the content taken down, but this will require the hiring of a lawyer. Google also provides options for getting information removed from a search, but this takes time as well. See, Kim Komando, \textit{How to Delete Yourself From the Internet}, January 25, 2013, http://www.usatoday.com/story/tech/columnist/komando/2013/01/25/komando-delete-yourself-internet/1852143/; for step-by-step tips, see, Sarah Downey, \textit{How to Delete Yourself From the Internet: A Guide to Doing the Impossible}, June 19, 2012, http://bostinno.streetwise.co/channels/how-to-delete-yourself-from-the-internet-a-guide-to-doing-the-impossible/.} Thus, even if a victim brings forth a successful invasion of privacy claim, the ensuing harm of posting the defamatory photo or video will continue, since there is no requirement that the content be taken down. Additionally, court documents with the victim’s name are considered public record and thus widely accessible due to the advent of online dockets, which in turn runs the risk of increasing exposure to the pictures and publicity to the case.\footnote{Susanna Lichter, \textit{Unwanted Exposure: Civil and Criminal Liability for Revenge Porn Hosts and Posters}, http://jolt.law.harvard.edu/digest/privacy/unwanted-exposure-civil-and-criminal-liability-for-revenge-porn-hosts-and-posters.}

\textbf{B. Digital Millennium Copyright Act}

On October 28, 1998, President Clinton signed into law the Digital Millennium Copyright Act ("DMCA") in order to protect copyright holders from the rampant copyright infringement occurring due to the increased usage and popularity of the
Internet.\textsuperscript{59} In essence, the DMCA imposes civil and criminal liability on “the production or dissemination of any technology that allows users to circumvent digital copyright protection…barred by the DMCA.”\textsuperscript{60} Importantly, the immunity granted by the CDA does not affect intellectual property law—including copyright law.\textsuperscript{61} Thus, ISPs may be held liable under the DMCA through “contributory copyright infringement”, which “occurs when one party, with the knowledge of another party…induces, causes, or materially contributes to the infringing conduct of another.”\textsuperscript{62} However, like the CDA, the DMCA provides immunity for ISPs if such providers did not know about the copyright infringement or if they comply with the notice and takedown procedures promulgated by Title II of the DMCA, known as OCILLA.\textsuperscript{63}

Although the DMCA is a viable option for revenge porn victims, there are some major catches. First, a victim who takes a “selfie”\textsuperscript{64} is the rights holder of the photo, and thus has the exclusive right to distribute and display the photo.\textsuperscript{65} As an exclusive rights holder, the victim can initiate the “notice and takedown procedures” outlined in OCILLA.


\textsuperscript{60} Id.


\textsuperscript{62} Gershwin Pub’g Corp. v. Columbia Artists Mgmt., Inc., 443 F.3d 1159, 1162 (2d Cir. 1971).

\textsuperscript{63} Ronneburger, \textit{Sex, Privacy, and Webpages: Creating A Legal Remedy for Victims of Porn 2.0}, at 25; (The notice and takedown procedure requires that a service provider “upon receive knowledge or awareness” of the infringing material, must “act expeditiously to remove, or disable access to, the material.” OCILLA, 17 U.S.C. § 512(c)(1)(A)(iii) (2006)).

\textsuperscript{64} “(2) A strange phenomenon in which the photographer is also the subject of the photograph, in a subversive twist on the traditional understanding of the photograph. Usually conducted because the subject cannot locate a suitable photographer to take the photo, like a friend.” http://www.urbandictionary.com/define.php?term=Selfie.

\textsuperscript{65} 17 U.S.C. § 201.
of the DMCA. However, many revenge porn websites have found methods to out-maneuver such takedown notices, such as hosting their sites on foreign web-servers—which are arguably outside U.S. jurisdiction—or hiding their server altogether. As a result, in order to establish where to send a DMCA takedown notice, the victim would have to sue the website and obtain a subpoena. This, in turn, presents additional problems for the victim. First, the victim would have to hire a lawyer in order to file a lawsuit, which is costly both in dollars and time. Second, the victim runs the risk of the “Streisand Effect,” thus drawing more attention to the material the victim is seeking to suppress. Additionally, as mentioned earlier, the DMCA only covers photos personal taken by the victim, not the poster.

Furthermore, websites such as ChillingEffects.org monitor DMCA takedown notices in order to assess their validity and provide “analysis of their claims to help recipients resist the chilling of legitimate activities (as well as understand when their activities are unlawful).” If websites, such as Google, are asked to remove specific links from their search results, they will send such demands to ChillingEffects.org, which in turn will post the takedown notice online. Intrigued, I went to ChillingEffects.org

66 See supra note 47.
68 Id.
69 Id.
70 The “Streisand Effect” is the phenomena where “by attempting to squelch information, you can inadvertently make it wildly popular.” Bill Mordan, The Streisand Effect, ACC Docket, June 2008, at 96.
71 See supra note 51.
and on the home page in the “Quick Search” box searched “revenge porn.” Thirteen matching notices resulted. When I clicked on the first link, there were nine different copyright claims with over nine hundred “allegedly infringing URLS” under each claim directing visitors to the website with the alleged infringing content.

Additionally, my search resulted with a DMCA takedown notice identifying a sender by name. The woman had sent the takedown notice to MyEx.com, a well-known revenge porn website, alleging that copyrighted work (a photo she took of herself) was posted by an ex-boyfriend without her permission. Within the notice was the posted link of the “allegedly infringing URL.” Thus, websites like ChillingEffects.org could potentially defer revenge porn victims from pursuing takedown notices since attention is directed straight to the alleged infringing content.

C. Implied and Express Contracts of Confidentiality

Legal scholars well versed in privacy law have suggested implied and express contracts of confidentiality regarding user-generated pornography.74 The United States Supreme Court has upheld an expectation of privacy in personal relationships with landmark decisions such as Griswold v. Connecticut75 and Lawrence v. Texas,76 thus displaying society’s commitment in preserving the privacy of what occurs in intimate and personal relationships.77 As a result, contracts of confidentiality could protect those in

74 Ariel Ronneburger, Sex, Privacy, and Webpages: Creating A Legal Remedy for Victims of Porn 2.0, Syracuse Sci. & Tech. L. Rep., Fall 2009, at 1, 19
75 381 U.S. 479 (1965) (striking down a state statute that prohibited the use of contraceptives); see id. at 485 (describing marital bedrooms as “sacred precincts”).
76 539 U.S. 558 (2003) (reversing a conviction for engaging in homosexual conduct in violation of a state statute); see id. at 578 (stating that individual decisions concerning intimacies of physical relationships are a form of “liberty” constitutionally protected by the due process clauses of the Fifth and Fourteenth Amendment).
“intimate relationships,”78 which often in this age of technology involves the sharing of private and often embarrassing information, including sexy pictures.79 Such implied contracts of confidentiality are created between the interactions of the couple while they are together and include any information shared.80 These contracts would only cover “the dissemination of private, embarrassing information through an instrument of mass communication,”81 such as the Internet. Accordingly, a breach of contract would only occur if the private information, such as a naked photo, was distributed on a type of widespread media, like the Internet.82

Alternatively, an express contract could be developed between two individuals in an intimate relationship.83 An express contract could lie out unambiguous terms defining the duties of the two individuals to keep information private, such as the following:

“The undersigned parties, for the valuable consideration of society, companionship and all of the other many services and benefits mutually conferred by intimate partners, enter into this agreement of confidentiality as part of an intimate relationship they have established. The parties agree … that the private information and acts be shared and take place in an atmosphere of mutual trust in which each party can rely on the other not to disclose to third parties private, [Private, embarrassing information] includes information relating to mental and physical health, sexual activities, personal finances, quirks and eccentricities, indiscretions, and immodest or sexually oriented photographs or video in any format.”84

Such express contracts would clearly provide the terms for each individual in an intimate relationship and prevent any interpretation difficulties inherent in implied contracts.85

78 Relationships not including “purely physical relationships, such as one-night stands.” Id. at 917.
79 Id. at 923-28.
80 Ronneburger, supra note 59, at 20.
81 McClurg, supra note 62, at 924.
82 Id.
83 Ronneburger, supra note 59, at 20.
84 Ronneburger, supra note 59, at 20 (citing Andrew J. McClurg, Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality, 74 U. Cin. L. Rev. 887, 923-28 (2006)).
85 Id.
Additionally, an express contract can provide in advance the type of damages available if a breach of contract occurs.\textsuperscript{86}

Despite the allure of creating an implied or express contract while in an intimate relationship, there are practical problems. First, even if recovery for breach of contract is available, the pictures are still plastered all over the Internet and websites do not have to remove the content at issue, since they are not a party to the contract. Further, compensation may not be sufficient to cover the harm of the information being shared. Additionally, there is nothing romantic about entering into an implied or express contract with a partner to whom an individual supposedly trusts. Practically speaking, it is unlikely two laymen will even think to enter into an implied or express contract protecting such information shared with a partner.

Apart from the practical problems associated with an implied or expressed contract is the legal implications of Section 230. “In virtually all civil litigation…state law has traditionally governed contracts….”\textsuperscript{87} However, the CDA explicitly preempts any state law: “[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.”\textsuperscript{88} Thus, any contract made between intimate partners will be void under Section 230 of the CDA.

\textbf{D. Criminalizing Revenge Porn}

Apart from an invasion of privacy actino, revenge porn victims may be able to find remedy in the realm of state criminal law that targets the poster of the defamatory content. Both New Jersey and California have successfully passed legislation to curtail

\begin{itemize}
\item \textsuperscript{86} \textit{Id.}
\item \textsuperscript{87} Michael E. Solimine, \textit{Enforcement and Interpretation of Settlements of Federal Civil Rights Actions}, 19 Rutgers L.J. 295, 326 (1988).
\item \textsuperscript{88} \textit{See supra} note 41.
\end{itemize}
revenge porn and punish the posters of such content. However, despite this seemingly colossal victory, revenge porn victims are often still without any remedy.

1. **New Jersey**

In January 2004, New Jersey passed a criminal invasion of privacy statute aimed to combat cyber-bullying.\(^89\) However, victims of revenge porn can potentially find relief through the statute. The law, aimed directly at posters of harmful content, criminalizes the photographing, filming, and distribution of 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.\(^90\) Significantly, this statute focuses on the disclosure of the photograph and not necessarily who took the actual photograph.

2. **California**

Most recently, California Governor Jerry Brown signed a bill on October 1, 2013 explicitly banning revenge porn. The bill states:

“[A]ny person who photographs or records by any means the image of the intimate body part or parts of another identifiable person, under circumstances where the parties agree or understand that the image shall remain private, and the person subsequently distributes the image taken, with the intent to cause serious emotional distress and the depicted persons suffers serious emotional distress…is guilty of disorderly conduct and subject to that same punishment.”\(^91\)

Despite specifically targeting perpetrators of revenge porn, it is likely that victims will not be protected. According to the Cyber Civil Rights Initiative, up to 80% of

\(^89\) Lichter, *supra* note 62

\(^90\) An actor commits a crime of the third degree if, knowing that he is not licensed or privileged to do so, he discloses any photograph, film, videotape, recording or any other reproduction of the image of another person whose intimate parts are exposed or who is engaged in an act of sexual penetration or sexual conduct, unless that person has consented to such disclosure. For purposes of this subsection, “disclose” means sell, manufacture, give, provide, lend, trade, mail, deliver, transfer, publish, distribute, circulate, disseminate, present, exhibit, advertise or offer…” N.J. Stat. Ann. § 2C:14-9(c)(West).

\(^91\) Cal. Penal Code § 647(4)(A) (West).
revenge porn victims have taken “selfies,” but the California statute “only applies when
the person accused of spreading the images online is the photographer.” Thus, that
means a vast majority of revenge porn victims are not covered by the California law.
Additionally, the statute requires “the intent to cause serious emotional distress,” which
excludes those who post the photographs solely for financial gains or “bragging rights.”

3. New York

In response to both New Jersey and California successfully passing statutes
providing relief to some revenge porn victims, Republic Senator Phil Boyle has proposed
a similar statute for New York. However, unlike California’s law that applies only to
the photographer spreading the content without the permission of the subject, New
York’s proposed legislation would include photos taken by the subject. Thus, because
New Jersey and California have taken affirmative steps to combat revenge porn, it
appears that other “game-changing” states like New York will follow suit to provide
relief for victims of revenge porn.

4. Section 230’s Impact on “Revenge Porn” State Laws

Despite these state laws, the exception found in Section 230(e)(1) applies only to
federal criminal violations. Thus, ISPs and website service providers are still immune
from any litigation stemming from the posted content at issue. The common thread

92 See supra note 59.
93 Heather Kelly, New California ‘Revenge Porn’ Law May Miss Some Victims, CNN, October 3,
94 Id.
95 Alex Hern, ‘Revenge Porn’ Websites Face New York State Ban, The Guardian, October 8, 2013,
96 See supra note 86.
97 Chris Welch, Following California’s Lead, New York Lawmakers Look to Criminalize ‘Revenge Porn,’
The Verge, October 7, 2013, http://www.theverge.com/2013/10/7/4813644/new-york-lawmakers-look-to-
criminalize-revenge-porn.
98 See supra note 49.
among the state laws aimed at revenge porn is they target the posters of the content, not
the ISPs. Because the 230(e)(1) exception does not pertain to state criminal laws, the
ISPs are under no duty to remove the content, regardless of the guilt of the poster. As a
result, victims are still faced with the issue of removing the content from websites where
it appears.

E. Additional Potential “Silver Lining” for Revenge Porn Victims

Although a majority of actions against website service providers fail due to the
broad implications of Section 230, a recent case in the Ninth Circuit brings about a
potential “silver lining” for revenge porn victims in the form of an exception to the rule.
In 2008, the Ninth Circuit was presented with a case regarding Roommates.com, a
roommate matching website, and the Fair Housing Act. Local housing councils alleged
a violation of the Act and state discrimination laws because the website required users to
describe their preferences in roommates and shared protected characteristics like gender
and sexual orientation. The court held that Section 230 liability did not apply because
the website acted as an information content provider.

By requiring users to complete questionnaires provided by Roommates.com, the
website contributed to the content that it placed on its website. As a result, the court
held that Section 230 liability did not shield online service providers from civil claims
when they “materially contribute” to the unlawfulness of the content.

---

99 Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1161 (9th Cir.
2008).
100 Id.
101 Id. at 1164.
102 Id. at 1167.
103 Id. at 1167-68.
that the CDA was not created to “create a lawless no-man’s-land on the Internet.”104 Thus, the Ninth Circuit broke away from the normal granting of Section 230 immunity to all ISPs.

Based on the Ninth Circuit holding, a website service provider does not have Section 230 immunity if it “materially contributed” to the illegal content.105 Thus, if the revenge porn website requires posters to answer questions about the person featured in the photograph or video, then arguably under the reasoning of the Ninth Circuit, immunity under Section 230 will not exist. Additionally, revenge porn victims may be able to argue that if a website actively seeks out the victim’s Facebook, LinkedIn, MySpace, Twitter, etc. accounts, then the site is materially contributing to the content and acting as an information content provider. However, the main problem with this argument is the court will first have to make the determination that the photo or video was acquired illegally—namely without the permission of the person taking the photo or through hacking.106

Another hurdle in this line of argument is the holding in Batzel v. Smith, a later Ninth Circuit case.107 In Batzel, the court extended Section 230 immunity beyond ISPs, holding that the alteration of content originally written or posted by a third-party, as well as proactively screening the third-party content before initial publication, still gave the ISPs Section 230 immunity.108 Thus, a revenge porn victim will not be able to rely on the argument that once the photo was submitted, the ISP altered it and thus materially

104 Id.
105 See supra, note 42.
106 See supra, note 60.
107 333 F.3d 1018 (9th Cir. 2003).
108 Id. at 1032.
contributed to the illegal content. Instead, the revenge porn victim will need to demonstrate that ultimately the ISP was not a “publisher” but rather an “information content provider” and contributed materially to the defamatory content by requiring certain information to be given, such as a link to the individual’s Facebook or Twitter account. Despite this seemingly promising “silver lining,” this Ninth Circuit case is the exception, rather than the rule.

IV. SUGGESTIONS IN FAVOR OF AMENDING SECTION 230

“Good laws lead to the making of better ones; bad ones bring about worse.”

Without a doubt, the CDA is a good law in that it allows for the “continued development of the Internet” and preserves the “vibrant and competitive free market” of ideas on the Web. Specifically, Section 230 allows for websites such as Yahoo! to provide a forum for users to comment on news stories, which in turn generates public discourse, without fear of liability for offensive or off-colored remarks. Without Section 230 immunity, sites like YouTube and Reddit, which largely consist of user-generated content, would cease to exist due to the risk of litigation stemming from the potentially defamatory content. Just as there is merit to Section 230 immunity, there is also a very real and detrimental downside. As the previous sections demonstrate, victims of revenge porn are faced with mountainous hurdles in order to seek any form of justice due to the broad immunity provisions of Section 230. Because of these major obstacles, the need for a “revenge porn” exception in Section 230 of the CDA becomes more readily apparent. Thus, a good law like the CDA must lead to the making of better ones—particularly those

109 Jean Jacques Rousseau (1712-1778).
111 Supra note 16.
that protect and give justice to victims who have unwillingly had nude photos of them plastered around the Internet.

A. Proposed Exception to Section 230 of the CDA

As a consequence to the major obstacles revenge porn victims face in seeking justice, I propose that Congress create an exception to Section 230 of the CDA. First, the exception would include a definition of revenge porn: the online posting of nude or sexual photographs of an individual without his or her consent. This definition would include content obtained through hacking or unbeknownst to the owner. Accordingly, website service providers, whose sites consist mainly of nude and sexually suggestive photos and videos, would be required to take down defamatory photos and videos within a fourteen-day period if they are put on notice that such photos or videos were distributed to the website without the permission of those featured in the photos or videos. My proposed exception would not require ISPs to self-regulate the content posted on the website, thus eliminating any sort of excuse that it would be unfeasible for the ISPs to remove all defamatory content posted because there is not enough time, resources, etc.

Rather, each website would be required to provide a link where takedown requests of unauthorized content could be submitted and reviewed within fourteen days. If the ISP refused to comply, judicial proceedings could potentially take years to resolve, thereby exacerbating the effect such content has on the lives of victims. To curb such detrimental effects caused by time and provide quick relief, the exception would provide for a court-ordered temporary removal until the court has come to a resolution regarding the merits of whether the alleged offending website had a legitimate justification for refusing to take down the content. If the court decides such justification for removal is
baseless or erroneous, the temporary removal of the content would become an order to permanently remove the offending post.

Once the ISP is put on notice of a legitimate takedown request, similar to the Digital Millennium Copyright Act ("DMCA"), the website must comply with the notice and takedown procedures created by the exception. After complying with the legitimate takedown notice, the ISP would be protected from any further liability stemming from the unauthorized content, such as civil claims targeting the poster of the content. The difference between the DMCA takedown procedure and my proposed exception is that victims would not be required to first sue the website in order to be granted a subpoena. Instead, websites that have made the conscious decision to allow the posting of content in the form of lewd photos and videos would take on the risk that such content posted was done without the permission of the original owner or subject of the photo/video—just as such websites take on the risk that those in the photos and videos are over the age of eighteen. Failure to comply with such legitimate takedown notices would result in either a court-ordered temporary shutdown of the website until the content is removed or joint liability stemming from the aforementioned state criminal laws targeting posters of revenge porn.

Additionally, because content can easily be shared among users, victims of revenge porn are often faced with the challenge of completely removing unauthorized content. Therefore, if a website features unauthorized content that has already been

112 See supra note 58.
114 See supra note 57.
subject to a takedown notice on a different website, the exception would require any additional website to comply with the takedown once put on notice. Constructing the exception in this way will put the burden on the victim to discover websites with the unauthorized content and, in turn, put them on notice. This would remove any self-regulating burdens on ISPs, while also providing relief for victims of revenge porn where the content has been shared among users to other similar websites.

By promulgating such a rule, a middle ground would be reached: ISPs would continue to enjoy the benefits resulting from the Section 230 safe harbor as long as they comply with the proposed takedown requirements. If ISPs refused to comply with the takedown requirement, benefits derived from the safe harbor would be stripped away indefinitely. Crafting the exception in such a way would retain the merits of Section 230, while also limiting the scope of the safe harbor.

2. Scope of the Proposed Exception

The proposed exception should be limited only to pornographic or sexually suggestive material defined as “revenge porn.”¹¹⁵ Such content is easily recognizable and affects a narrow class of websites—specifically websites such as MyEx.com that encourage the posting of revenge porn material. By narrowly affecting a certain class of websites, the exception would not be over-inclusive—it would be directed exclusively towards the antagonists and proprietors of revenge porn, thus fortifying the purpose of the exception.

In cases of defamation and other related causes of action, Section 230 would be rendered completely useless since Congress promulgated the safe harbor to alleviate the

¹¹⁵ See supra note 7.
burden imposed on ISPs to self-regulate and police all of the content found on user-generated websites. If applicable to defamation and similar causes of action, the exception would encompass virtually every website that allows user-generated content, such as “comment” sections. This expansive application of the exception would severely burden websites by forcing a response to every takedown notice—regardless of the legitimacy of such claims. Although rude and disparaging content is pervasive throughout the Internet, the risk of silencing legitimate speech is too high and such an application would cause the “chilling effect” Congress sought to avoid by creating the safe harbors of Section 230 of the CDA.\(^\text{116}\)

3. First Amendment Considerations

Proponents of ISP blanket immunity of Section 230 will argue that such an exception will result in over-deterrence and cause needless removal of acceptable content. However, there is always the possibility that over-deterrence will result when any law aims to prevent destructive behavior.\(^\text{117}\) Well-balanced policies are not immune to over-deterrence in certain occasions and under-deterrence in others.\(^\text{118}\) Rather, “the acceptability of those errors depends on the values we attach to the problematic conduct and to the potential harm.”\(^\text{119}\) The line between our Internet activities and real world activities is growing thinner as technology progresses. Thus, there is an increasing need of laws that will protect both our “online” lives and “real world” lives.

As a result, it is important to understand the First Amendment protects freedom of expression, which serves several important purposes: to maximize public discourse, the

\(^{116}\) Supra note 19.

\(^{117}\) Danielle Keats Citron, Cyber Civil Rights, 89 B.U. L. Rev. 61, 120 (2009).

\(^{118}\) Id.

\(^{119}\) Id. at 121.
First Amendment protects those who disagree with the majority; creates an ideal forum with the goal of achieving the exchange of robust debate and ideas; and allows our democracy to work through the free exchange of ideas and opinions.\textsuperscript{120} Such expression allows for the facilitation of ideas and information, which are both profound functions in a self-governing, democratic citizenry.\textsuperscript{121} Thus, the First Amendment protects both popular and unpopular speech, with the aim of cultivating the free flowing exchange of ideas and information to better our society.

However, long-held precedent has established that speech categorized as “defamatory” or “obscene” is generally left unprotected by the First Amendment, namely because such speech is not conducive to a democratic society.\textsuperscript{122} Thus, damaging photographs, like the ones posted onto revenge porn websites, do not generate ideas in popular culture or enforce positive social norms.\textsuperscript{123} Rather, such harmful content perpetuates serious social harm for revenge porn victims in the form of separation of the victim from the community, subjection to stalking and harassment, lost jobs, ruined reputation, and even suicide.\textsuperscript{124}

Although the United States Supreme Court struck down as unconstitutional under the First Amendment parts of the CDA addressing liability for indecent materials exposed to minors,\textsuperscript{125} the provisions guaranteeing broad immunities to ISPs remain intact.\textsuperscript{126} As

\begin{footnotes}
\item[120] Laurence H. Tribe, \textit{American Constitutional Law} 785-89 (2d ed. 1988).
\item[121] Tribe, \textit{supra} note 42, at 577.
\item[125] See Reno v. ACLU, 521 U.S. 844 (1997).
\end{footnotes}
a result, when discussing potential reasons for changing Section 230, proponents of the blanket immunity clause are quick to hide behind the guarantees of the First Amendment. Specifically, those who are in favor of blanket immunity fear that a lack of such a provision will result in over-deterrence, thus prompting website operators to automatically remove posts that may stir complaints—even if frivolous—causing the chilling of speech.127

However, my exception does not completely invalidate the safe harbors of Section 230, nor does it make revenge porn illegal. Rather, it provides a narrow exception exclusively targeting the unauthorized posting of content considered to be revenge porn. The proposed exception would be in violation of the First Amendment only if it impermissibly impeded the facilitation of the free flow and exchange of ideas required of a well-functioning democracy. Instead, the proposed exception is geared exclusively at providing a remedy for revenge porn. Revenge porn, because of its harmful and detrimental effects on society, is well outside the protections of the First Amendment.

Uncontestable is the notion that the Internet is a forum in which public discourse can and should take place. The Internet provides numerous opportunities through blogs, forums, message boards, and instant message to discuss a wide variety of topics ranging from the raising of alpacas to current events—all with the aim of providing a forum for the free flow exchange of ideas and opinions. When forums such as the Internet exist, it is equally irrefutable that First Amendment protections should apply to encourage the dissemination of ideas and information, regardless of popularity, which are all pertinent to the development of a democratic society. However, the evolution of the Internet as

both an arena of robust debate and back alley of vicious attacks, such as revenge porn, calls for Congress to protect users.

In a 2005 Pew Internet & American Life Project study, researchers found that the proportion of the Internet users participating in online discussions plunged from twenty-eight percent in 2000 to seventeen percent in 2005.\footnote{Deborah Fallows, Pew Internet & American Life Project, How Women and Men Use the Internet 14 (2005), available at http://www.pewinternet.org/~/media//Files/Reports/2005/PIP_Women_and_Men_online.pdf.pdf.} Further research discovered that the sharp decline was contributed to a “large exodus of women.”\footnote{Id.} If the argument for First Amendment protection is to prevent the chilling of speech, refusing to pass laws protecting revenge porn victims due to First Amendment considerations is wholly counterintuitive. Rather, speech is chilled by victims of revenge porn—both male and female—who are afraid to access the Internet, or do so limitedly, in fear of facing unwanted photos and videos splashed all over the Internet.

V. CONCLUSION

Despite the merits behind Section 230 of the CDA “to promote the continued development of the Internet and other interactive computer services and other interactive media”\footnote{47 U.S.C.A. § 230(b)(1) (West).} and “to preserve the vibrant and competitive free market that presently exits for the Internet and other interactive computer services, unfettered by Federal or State regulation,”\footnote{Id. at § 230(b)(2).} the broad liability given to ISPs presents very real problems and consequences for revenge porn victims. Notwithstanding common law actions, state “revenge porn” laws, and the DMCA, revenge porn victims need additional protection that will mitigate the damages of defamatory content.
Thus, Section 230 of the CDA should be amended to provide protection to revenge porn victims through obligatory takedown procedures once notice is given to ISPs. Although First Amendment concerns are understandable, such malicious content serves no purpose in cultivating the free flow of speech and ideas necessary for a democratic society. Our laws exist to provide order and protection for citizens in society—including citizens online. Because of the growing pervasiveness of revenge porn, lawmakers have an obligation to amend Section 230 of the CDA to protect victims and mitigate the harms stemming from the public disclosure of such private information.

\[132 \text{ See supra note 107.}\]