Online Gendered Harassment and Violence

Naming the Harm and Punishing the Behavior

by

Madeleine Rose Kimble

A senior thesis submitted to the Department of Communication Studies at The University of Michigan in partial fulfillment of a Bachelor of Arts degree (Honors)

April 2016

Thesis Committee:

Honors Faculty Advisor Professor Scott Campbell

Honors Thesis Advisor Professor Faith Sparr

Abstract

The purpose of this study was to examine three forms of online gendered harassment and violence aimed towards women, and current laws' ineffectiveness in addressing their harm, in order to propose legal reformations. The need for new efficacious laws addressing women's gendered harm online is supported by data detailing the severity of cyberbullying, online sexual harassment and cyberstalking cases across the country—and their detrimental effect on victims' online and offline lives. This study will first examine the similarities between online gendered harms and their traditional offline counterparts, highlighting how past trivialization of gendered crimes are being applied now. By defining the behaviors and their harm, and providing examples through victims' experiences, it will then be determined that the many forms of online gendered harassment and violence are not inconsequential Internet communications. However, there are aspects that pose a challenge to addressing victims' harm, such as the unique characteristics of the Internet and ineffective civil, criminal, and Internet laws. By analyzing gaps in these policies, it will be determined where state and federal legislation can be improved. States and the federal government can enact successful and effective laws by addressing the unique characteristics of abusive online gendered behaviors and Internet communications, and by including comprehensive legal requirements and definitions.

Keywords: civil torts, credible threat, criminal law, cyberbullying, cyberspace, cyberstalking, defamation, intent, intentional infliction of emotional distress, online sexual harassment, Section 230 of the Communications Decency Act

Acknowledgements

I would first like to express my deepest gratitude to my Honors Faculty Advisor Professor Scott Campbell for his excellent guidance, caring, patience, and providing me with an excellent atmosphere for doing research. Thank you for encouraging me to push myself and for steadfastly enduring my seemingly endless barrage of emails and re-edits throughout this process. I could not have developed this thesis without your help.

To my Honors Thesis Advisor Professor Faith Sparr, thank you for your patient guidance and for being a constant source of reassurance and inspiration. Your door was always open whenever I ran into trouble or had a question about my research and understanding of the law. Thank you for making this endeavor a productive and fun learning experience. I could not have imagined having a better mentor.

Finally, I must recognize my amazing family network for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. Thank you for your patience in listening to me talk non-stop about my topic over the past year, and giving me your attentive ears. To my parents, thank you for encouraging me to do more than I thought I could, and for always having my best interest at heart. You are always there for me. This accomplishment would not have been possible without you.

Thank you all.

Table of Contents

Introduction

Online harassment and violence towards women has become a widespread problem with the advance of technology. Stereotypical and detrimental attitudes towards women are strongly visible in online spaces, despite the physical absence of users (Stoleru, 2014, p.96). The harms pushed onto women can be severe, affecting their mental, emotional, and even financial health. Online, 37% of women report experiencing gendered abuse, including exclusion from online domains, revenge pornography, stalking, and threats of sexual violence and death (Duggan et al., 2014, p.5). Violence and harassment against women is by no means new. Historically, the harms suffered by women—such as sexual harassment, stalking, and rape—have been prevalent in many western societies, and were often met with trivialization or dismissal from the predominantly patriarchal society. The difference between online and offline harms however, is how they have been addressed. Activists, lawyers, and everyday citizens in the 1970s to 90s helped gain the acknowledgement of the courts that the offline harms suffered by women were not only real, but serious. This prompted new legislation that both prohibited and penalized gendered harassment and violence in both public and private spaces. But despite the same seriousness of the harms inflicted upon women in online spaces, calls for the prohibition and punishment of gendered harassment and violence in cyberspace has been slow to start, if at all.

Harassment and violence has become a common part of the Internet experience. In a study of online harassment in 2014, 73% of adult Internet users saw someone being harassed online —such as witnessing comments in which someone was physically threatened or sexually harassed— while 40% experienced it personally (Duggan et al., 2014, p.2). The study also showed that women were more likely to experience certain severe types of harassment and violence online at disproportionately high levels compared to their male counterparts. These

experiences included being stalked and sexually harassed—26% of women compared to 7% of men, and 25% of women compared to 13% men respectively (Duggan et al. 2014, p.3-4)[1]. Women between the ages of 18-24 were also more than twice as likely as their older cohorts (25-29 years old) to be sexually harassed, stalked, and physically threatened for long periods of time online (Duggan et al., 2014, p.14-15). Whether the perpetrator is reducing women to their sexualized body parts, threatening rape, or invoking gender demeaning stereotypes, they make clear that women are targeted due to their gender (Citron, 2009, p.384).

Researchers have framed these abusive behaviors in multiple ways. Nicola Henry and Anastasia Powell (2015) characterized gendered behaviors through their framework of "Technology-Facilitated Sexual Violence and Harassment ('TFSV')". Defined as the collective range of "criminal, civil, and otherwise harmful sexually aggressive behaviors perpetrated against women with the aid or use of technology", TFSV embodied six different behaviors, including online sexual harassment, cyberstalking, and virtual rape (p.759). Others, such as Trevor Milford (2013), defined the behaviors more broadly though the framework called "Cyber [Gender] Harassment", defined as "any instance where there is a power imbalance favoring a perpetrator over a [female] victim" (p.2). For the purpose of this study, a new framework for analyzing gendered online abuse has been developed. Drawing from Henry and Powell's (2015) and Milford's (2013) theories, this study advances a framework that will be called "Online Gendered Harassment and Violence" or "OGHV". This term will be used to describe the range of criminal, civil, emotional and physical harm caused by aggressive gendered behaviors. OGHV behaviors are categorized according to four different forms: cyberbullying, online sexual

[1] It was only when being called offensive names or being purposefully embarrassed that men experienced more abuse than women, but only with a difference of 1-2%.

harassment, cyberstalking, and cyber rape. While these abuses occur to both men and women, research suggests that women are disproportionately the targets of such abuse in cyberspace, and so this theory applies specifically to women.

The case of Anita Sarkeesian is a prime example of the severity of OGHV. For years, Sarkeesian ran a YouTube video series called "Feminist Frequency" in which she analyzed pop culture and the place of women in it from a feminist perspective. In 2012, Sarkeesian began a kickstarter campaign to raise funds for her new project *Tropes vs. Women in Video Games*. Within a day of posting a video about the forthcoming project on YouTube, hundreds of sexist comments flooded her video-sharing site, and by the end of the month Sarkeesian had become the target of a cyber mob. Harassers vandalized her Wikipedia page, editing the text to call her expletive names such as "cunt", and changed the external links to "re-reroute to porn sites and adding a drawing of a woman with a man's penis in her mouth captioned with 'Daily Activities'" (Sarkeesian, 2012b, para.5). Hackers attempted to steal the passwords to her website and social media accounts, reported her Twitter and YouTube accounts as "terrorism", "hate speech", and "spam" (Sarkeesian, 2012a, para.2) and even spread her address and telephone number around the Net. Sarkeesian received thousands of messages through Facebook and Twitter with comments that ranged from sexist kitchen jokes to threats of violence, sexual assault, and death. Images and drawings of Sarkeesian's likeness being raped or sexually assaulted and humiliated were also distributed on online forums (Sarkeesian, 2012c, para.10-11), and one perpetrator developed a game that allowed players to "Beat Up Anita Sarkeesian" by revealing a more bruised and bloodied photo of her with each click.

The consequences of OGHV have damaging effects to both the online and offline lives of female victims. Anorexia nervosa and depression are common ailments for individuals who are

harassed online (Citron & Franks, 2014, p.351), and a study from Australia suggests that many online stalking and sexual harassment victims display at least one symptom of post-traumatic stress disorder, whether or not they have been physically assaulted (Quarmby, 2014, para.12). Other studies have shown that victims "become more fearful, distrustful of others, can develop physical illnesses and even become suicidal" (Quarmby, 2014, para.12). To avoid further abuse, targeted individuals often withdraw from online activities, costing them online exposure that could help in finding and gaining employment (Citron & Franks, 2014, p.352). Abuse that begins online can also extend offline when victims experience menacing phone calls, stalking, and even physical assault. Identity theft and physical safety can also become an issue as victims' social security numbers, telephone numbers, and addresses are distributed across the web. Consequences from Sarkeesian's online harassment even followed her years later in her offline life. In October of 2014, Sarkeesian was forced to cancel a speech at Utah State University when, the day before, members of the university administration received an email warning that a shooting massacre would be carried out at the event (Wingfield, 2014, para.2).

Despite the serious effects of OGHV, few victims come forward to report attacks due to public trivialization of the issue. Responses to online harassment and violence claims have been met with outright dismissal, or counsel that the abuse is merely a juvenile "prank" and that victims are being overly-sensitive (Citron, 2009, p.375). This societal trivialization has made it harder to seek legal protections against perpetrators as law enforcement fails to take the issue seriously, and are not properly trained in how to address such situations. Complications also arise when commentators claim that these messages, though distasteful and offensive, are protected under the First Amendment. Due to indistinct lines between which comments can be considered legitimate threats, many offenders have avoided legal action by claiming that their words

constituted as jokes or "*trolling*". The few laws that do exist to combat online harassment and violence are also hard to enforce, and prosecuted individuals face minimal charges and fines for misdemeanors—a miniscule consequence that does little to curb the abuse.

Motivated by this trivialization and lack of appropriate response, this study aims to show that OGHV towards women is not a mere Internet "prank", but instead prosecutable abuses that have found their way into the digital realm, and can be just as (if not more) damaging due to the lack of traditional constraints and boundaries. This study aims to deepen the understanding of what online gendered harassment and violence towards women is, the inadequacies of the current legal system to handle such cases, and the opportunities for curbing it from a policy perspective. Part I of this study will explore the history and harms of offline gendered harassment and violence and detail the steps that led to legal reforms. This will then be compared and contrasted to modern forms of OGHV, including its trivialization. Part II will name and describe the abusive behaviors, accompanied by examples of individual's experiences, to gain insight into the different forms and severity of OGHV. Part III will then discuss current laws to analyze policy gaps that allow for such abuse to occur with little intervention or punishment. In Part IV, suggestions will be made for policy changes with the goal of providing better legal recourse for victims. Conclusions and suggestions for further study will then be expressed in Part V.

Analytic Categories

Behavior selection rationale. Within this study, three of the four behaviors of OGHV will be analyzed: cyberbullying, online sexual harassment, and cyberstalking[2].

[2] Although cyber rape is still included within the OGHV framework, due to its recent emergence in cyberspace and its more limited range of victims and legal reparations, it currently lies outside the scope of this study.

Cyberbullying, a practice predominately associated with and perpetrated by children, has been included into OGHV behaviors and analysis for two reasons. First, statistics show that a majority of cyberbullying victims are female, and that gender and sexual harassment are the most prevalent forms of cyberbullying (Lightburn, 2009, p.14; Shariff & Gouin, 2006, p.4). Second, while cyberbullying may be committed by children, the types of behavior and reactions to it can be considered the precursor to future gendered harassment and violence online. Children involved in gendered cyberbullying can be shaped by the experience, and how schools and administrations handle these early signs of concerning adult behavior can set a precedent for expected consequences of adult OGHV. To analyze and find solutions for preventing these acts is an attempt to stop future OGHV perpetrators from being created, and empower those individuals who may become victims to expect more from authorities. Online sexual harassment and cyberstalking have been included due to their offline counterparts' historic prevalence in women's lives. Offline stalking and sexual harassment have plagued women for centuries, and though recent laws have worked to combat the practices, it is important to show how the new digital medium is allowing for the behaviors to continue—in some cases unencumbered.

Policy selection process rationale. Despite the vast number of criminal and civil actions that could be applied to OGHV cases, this study has limited analysis to select civil torts and the inadequate handling of online harassment and violence by online and offline authorities. In order, this study will examine: 1) defamation torts; 2) intentional infliction of emotional distress torts; 3) authorities' implementation of criminal law; and 4) the protection of site administrators under Section 230 of the Communications Decency Act.

Civil torts, wrongs that result in an injury or harm that constitute the basis for a claim by the injured party, were chosen to be included due to their common use in OGHV cases. As not

all forms of OGHV are considered criminal in certain states, many times victims turn to civil torts in an attempt to find justice against their abuser. As such, it is important to note why civil torts fail to provide the appropriate justice. The specific civil torts mentioned within this study—defamation and intentional infliction of emotional distress—were chosen for multiple reasons. First, each tort can be used against perpetrators in at least one of the three OGHV categories, allowing for a comprehensive understanding of the legal problems faced within each situation. Second, these torts were those that appeared the most in the examined literature, and so appeared to be the most important torts in victims' fight against OGHV.

The focus on issues between victims of OGHV and police and prosecutor's implementation of criminal law was chosen to be included due to their influence in validating victims fears and prosecuting offenders. Although OGHV behaviors occur online, prosecuting perpetrators involves offline intervention, and thus requires the cooperation of authorities. To the credit of law enforcement, many agencies have begun developing their own cyber crime units. However, a report by the Police Executive Research Forum in 2014 showed that police still have problems when it comes to prosecuting perpetrators of cyber crimes. Some departments have yet to create a cyber crime division, while officers may remain untrained in how to handle the new medium in such traditional cases (Wexler, 2014, p.10). Many cyber crime units also only focus on bigger crimes, such as data theft and fraud, rather than individual cases of harassment and violence (Wexler, 2014, p.2). Jurisdictional boundaries and a lack of understanding of new digital mediums were also cited as reoccurring problems for police investigations and prosecution of perpetrators. It is for these reasons that focus must be turned towards police and the current prosecution scheme so as to see what obstacles currently stand in their way, and what can be improved. Thus, this study focuses on the inadequacies of police and prosecution schemes

through the problems of jurisdiction and lack of technological knowledge and training.

Although police investigations are only present in criminal cases, specific criminal charges were not chosen to be included within the policy section of this study for two reasons. First, federal and state governments have their own criminal laws in regards to OGHV behavior. With more than fifty state and federal crimes that perpetrators could theoretically be charged with, dissecting specific statutes was beyond the scope and resources of this study. Instead, due to the commonality of requirements for criminal prosecutions among federal and state criminal policies, it was deemed that showing the *common* loopholes of such laws would be a more feasible approach. This study therefore focused on the requirements of "credible threat" and "intent" of the perpetrator due to their common appearance in state and federal criminal law and academic literature. Second, throughout the examined literature, few cases involved perpetrators being prosecuted and convicted of criminal offenses. This may be due to OGHV cases not appearing criminally dangerous to the courts due to the separation of the victim and perpetrator via the medium. Further, these gaps in criminal law, accompanied by barriers posed to authorities, evidence of criminal behavior may not have been gathered or the actions of the perpetrators may not have been considered to be illegal. However, this does not mean that there is no possibility for charging perpetrators with criminal offenses. Therefore, possible criminal charges shall be discussed in section IV along with other possible legal remedies.

Finally, barriers posed by Internet service providers and website administrators' use of Section 230 of the Communications Decency Act was included due to the large influence these parties possess in preventing violent gendered behaviors online. As there are no law enforcement officials patrolling cyberspace, website providers and administrators are the closest things to authority figures that cyberspace can have. They set the rules for specific spaces online, monitor,

remove, and allow content to be seen by community members, and possess the ability to ban certain users from a space—one of the most powerful weapons in keeping community members in line. To overlook the roles website providers and administrators play in preventing—or in many cases refusing to prevent—OGHV behaviors would be to accept the idea of a cyber "wild west" norm. This would also ignore the possibility of consequences for perpetrators and relief for victims that can be enacted online without the need for law enforcement intervention should the tools be utilized properly.

I. Gendered Harms towards Women: Then and Now

Harassment and Violence towards Women in Offline-Space

Harassment and violence towards women is not a new phenomenon confined to online formats. For centuries, harms against women were not only considered socially acceptable, but legal. It was not until the last few decades that these issues came to the attention of and garnered concern from U.S. lawmakers, prompting legal reforms that prohibited and punished such behavior. Though not completely foolproof, these reforms made harassing and violent behavior deviant, pushing those who enacted them to the fringes of society. With the advent of technology however, these socially unacceptable behaviors have migrated to cyberspace where there are less restrictions and enforcement on social norms. To understand the best way to combat and regulate OGHV harms in cyberspace then, it is important to analyze how such behaviors were first combatted offline.

Gendered harassment and violence towards women in the offline world reflected the views of women's place within society, placing them at both a legal and societal disadvantage. Crimes that were suffered primarily by women were often met with extensive legal barriers when brought to prosecution. For example, women who claimed they were raped were required to

provide witness corroboration and evidence of "utmost physical resistance", which made it difficult to convict men of rape (Citron, 2009, p.392). The reason for this, as Robin West (2011) explained, was because "women's injuries [were] often not recognized or compensated as *injuries* by the legal culture" (p.150). According to West, this was due to "women often [finding] painful the same event or condition that men find pleasurable; a man may experience at worst offensive, and at best stimulating, that which a woman finds debilitating, dehumanizing or even life-threatening; and that many men are simply oblivious to the conditions that women find frightening and painful" (West, 2011, p.149-150). Overall, West (2011) argued that the blanket dismissal of women's gender-specific suffering by the legal culture partly reflected how the harms were not understood because of their difference to the harms men faced, and that women effectively suffer differently (p.153). It was this difference and the inability of women to name their harm that created legal barriers for gendered crimes, while at the same time not mandating special requirements of proof for crimes that both genders faced equally. Thus, criminal law "historically targeted gender-specific harms only to the extent that they resembled harms suffered by men" (Citron, 2009, p.392).

Sexual harassment, domestic violence, and stalking were three such gendered forms of harassment and violence towards women that were continually dismissed by society and the courts. Although an exact definition of sexual harassment has not been specified, multiple definitions converge on three key areas, which indicates a basic level of agreement of describing sexual harassment as 1) unwelcome or unsolicited attention; 2) the harassment is viewed as sexual in nature; and 3) the acts are appraised as deliberate or repeated (Siddiqui, 1998, p.87). Sexual harassment has been present within society since antiquity, but no term existed to describe it until the 1970s. The brutality of domestic violence—the willful intimidation, physical

assault, battery, sexual assault, and/or other abusive behavior perpetrated by one intimate partner against another (National Coalition Against Domestic Violence, "n.d", para.1)—was also ignored or downplayed for over 200 years, with many considering it a "private" matter of the home. Stalking, the constellation of behaviors in which one individual inflicts on another repeated unwanted intrusions and communications, was not recognized as a significant crime until the mid-1990s (Spitzberg & Hoobler, 2002, p.72-73). Although commonly associated with incidents of domestic abuse (King-Ries, 2011, p.136), after more than two decades of research there is still no solid definition of offline stalking agreed upon in academic literature (Ahlgrim, 2015, p.2) and a consensus has yet to be reached among the states about the appropriate legal punishments. While men also experienced these forms of harassment, throughout history the primary victims of such violence were women. Such complaints of harassment and violence were therefore considered "women's problems" rather than societal ailments.

Women's complaints against such abuse were usually met with indifference, with commentators and authorities trivializing women's suffering along several lines. First, harms towards women were dismissed as "silly" everyday behaviors or a form of innocuous teasing. Workplace sexual harassment was one such behavior where complaints were met with the rationale that it was "normal" behavior for men, and that they were just "playfully flirting". Employers and officers would dismiss the harassment with a "boys will be boys" mentality that treated men's unwanted sexual advances as natural and women's resistance as abnormal. In cases where women were granted a trial, judges would also display this mentality, stating, as one court did that "the attraction of males to females…is a natural sexual phenomenon and it is probable that this attraction plays at least a subtle part in most personal decisions" (Citron, 2009, p.393). Normalizing sexual harassment put the power of sexual encounters predominantly in men's

hands rather than distribute the power to initiate, accept, and reject sexual encounters between both parties.

Stalking was also normalized by many, including police, as a nuisance rather than a crime (Hall, 1997, p.16). Before the 1970s, obtaining help for stalking cases was hard for women as stalking was not classified as an illegal activity. For many officers, stalking cases appeared insignificant as they often manifested as violations of protective orders or harassing phone calls, and were thus categorized as low priority for response. Trivialization of the problem was also a common occurrence as victims claimed that officer's response to their victimization was insensitive and inappropriate. Officers were also accused of blaming the victim, and that the criminal justice system's lackluster response only encouraged the stalker to defer responsibility for their actions and become bolder in the future (Hall, 1997, p.81-82). The cases were also considered low priority as, often, nothing physically had happened yet to the victim. Such blasé reactions to stalking cases could be met with tragedy. As stated by one judge after the murder of five women by their stalkers; "In some of the cases, the police told the women there was nothing they could do until the man committed a criminal act. By then it was too late" (Hall, 1997, p.22-23). In these cases, society refused to recognize emotional distress as a form of violence, and normalized the actions of perpetrators as innocuous inconveniences.

Second, society refused to recognize the harms done to women when it was felt that they could avoid the injury themselves, an argument that allowed domestic violence to occur almost unhindered socially and legally for decades. Judges, caseworkers, and psychiatrists treated battered women as the responsible parties for their abuse. Many advised the women that they could mitigate the harm themselves if they only "improved their appearance", or that they suffered from "feminine masochism" that propelled their husbands into beating them in response

to their nagging (Citron, 2014, p.82). Commenters also claimed that if the abuse suffered by women was so extreme, then wives could simply leave their husbands to escape the abuse. Judges dismissed assault cases if the abused spouse did not leave their batterer, and required women to prove that they had done everything to rid themselves of their abusive partners—including divorce—to warrant taking the assault seriously (Citron, 2014, p.82). The same ideology was also applied towards sexual harassment in the workplace. Commentators claimed that female employees "asked" supervisors and co-workers to proposition them by dressing provocatively, and courts legitimized this by permitting employers to defeat sexual harassment claims with proof that female employees "invited" the sexual advances (Citron, 2014, p.81). By this reasoning, women were in charge of making sure they were not sexually harassed by controlling what they wore and how they acted around male co-workers. When vocalizing their complaints, women were told to change their supervisors, jobs, or quit if the treatment in the workplace was too uncomfortable.

Finally, many refused to recognize these harms due to what they perceived as an environment's unique norms. With domestic violence, officers and judges refused to look into what they considered private family matters, considering a man's battering of his wife as protected as part of the "private sphere of family life" (Citron, 2009, p.394). Police officers were instructed to treat wife beating as a "private" matter that was best to be dealt with within the home (Rockwood, 1977, p.19), and some even viewed arrests in wife battering cases as attacks on the family unit (Rambo, 2003, p.35). The same attitude was aimed towards businesses when it involved sexual harassment. Considered to be a perk of the job for men, sexual harassment complaints were dismissed by the courts because "employers were expected to deal with them" (Citron, 2014, p.82).

This oppressive legal system has since changed in the last four decades as the aggressive gendered behaviors and their harms have acquired names. Starting in the 1970s and 80s, the women's liberation movement brought attention to gendered harassment and violence through legislative and grassroots activism, positioning the issues as problems for society rather than just women. This was done through naming the behaviors, such as coining the terms "sexual harassment" and "domestic violence" as a way to describe the pain suffered by women. According to West (2011); "If we want to enlist the aid of the larger legal culture, the feel of the gender-specific pain must be described before we can ever hope to communicate its magnitude" (p.153). By lacking a name for the harm and thus a linguistic reality, the victim as well as the perpetrator turn the harm into something else, such as punishment (domestic violence), flattery (sexual harassment), or unconscious pleasure (stalking) (West, 2011, p.153). To convince society and the lawmakers that the pain from gendered harassment and violence is legitimate, "we must give voice to the hurting self…even when that hurting self voices 'trivial' complaints; even when the hurting self is ambivalent toward the harm and even when (especially when) the hurting self is talking a language not heard in public discourse" (West, 2001, p.154). In order to combat the gendered harms faced by women, activists and members of the women's movement did just this.

Regarding sexual harassment in the workplace, Catharine MacKinnon, then a Yale law student, was first to coin the term "sexual harassment" in the draft of her book *Sexual Harassment of Working Women* in 1979. MacKinnon used the new term to galvanize efforts to delegitimize sexual harassment by claiming that the subordination of women to men within the workplace through sexual harassment constituted as a form of sex discrimination;

> "It is mysterious how women can fully participate in national life when the law continues to reinforce 'suitable' separate (… inferior) spheres of work, recognize

> ‘unalterable’ differences in personality, and enforce dual standards of behavior—unless a ‘separate but equal’ form of participation in national life is presumed to define ‘full participation’ for women” (MacKinnon, 1979, p.136).

Efforts to eradicate discrimination within the workforce had been addressed previously in Title VII of the Civil Rights Act of 1964, which included prohibiting sex discrimination—but sexual harassment had never been considered to fall under such protections. Lawyers used MacKinnon’s arguments to bring sexual harassment cases to court, and reasoned that sexual harassment fell under Title VII protections (Geare, 1998, p.244). Activists rallied to teach employers about sexual harassment and adopt anti-harassment policies, and provided information about local laws and referrals to crisis counselors (Citron, 2014, p.98).

The movement to provide legal recourse for victims of domestic violence started in much the same way when advocates coined the term (“domestic violence”) in the 70s. By giving a name to the behavior, advocates brought to light wife battering as a societal problem rather than a private family matter. Advocates emphasized that such behavior was not a private practice of “disciplining” wives’ unruly behavior, but a form of violence meant to subjugate and oppress. Victims came forward to speak about their experiences to both the media and courts, detailing their physical, mental and emotional harm. Feminist activists and lawmakers engaged in helping individual women obtain housing and public benefits to escape their abusers, and sought system-wide change with litigation challenging the legal system’s inattention to domestic violence (Citron, 2014, p.98-99). Advocates talked to the press about obstacles women faced when attempting to leave their abusers, including the fear of being unable to financially support themselves (Rambo, 2003, p.37), and of being subjected to more violence should their partner follow them.

The physical, mental, and emotional tolls of stalking have also since been recognized. In 1990, after the murders of five women in Orange County within a six-week period—all of whom were killed by their male stalkers—California became the first state to initiate anti-stalking laws, with similar actions eventually spreading to all fifty states (Ahlgrim, 2015, p.1; Hall, 1997, p.22). For the first time, harassment through obsessive behavior was taken seriously. Courts began attaching serious penalties to actions that occur early in an escalating series of events, prompting earlier action from authorities rather than waiting until physical harm or death occurred (Hall, 1997, p.23). Slowly, the courts began to acknowledge the arguments discrediting the reasons behind society's protection of sexual harassment, domestic violence, and stalking, and increasingly issued rulings punishing such behavior.

While offline gendered harassment has not been eradicated by any means, naming the harms and providing adequate legal redress for victims has provided a network of support that has helped many victims escape their abusers, and has created work and public environments where women can feel more comfortable in performing their daily activities.

Cyber Harassment and Violence towards Women

But should gendered harassment and violence offline be viewed in the same light when carried out online? The answer is complicated.

In simplest terms, OGHV is the same discrimination and abuse perpetrated against women offline, but repackaged and transmitted over a different medium. Whereas once an employer physically harassed an employee through inappropriate touching, gestures, or conversations, these communications are now sent through electronic devices and formats such as emails, texts, pictures, and videos. Stalkers can log on to a woman's social media account and digitally follow her throughout the day, discovering the target's private information with just a

click of a button. Threats of physical violence are common in OGHV communications, routinely involving threats of sexual assault, mutilation, and rape—some of which perpetrators attempt to carry out offline (Citron & Franks, 2014, p.351). According to a study in 2014, 37% of women experienced at least one form of online harassment and violence[3], and were still particularly vulnerable to sexual harassment and stalking (Duggan et al., 2014, p.5). The study found that 26% of women who claimed they experienced harassing and violent behavior were stalked online, and 25% were the target of online sexual harassment. In addition, they did not escape the heightened rates of physical threats and sustained harassment common in offline spaces (Duggan et al., 2014, p.3-4). Thus, there is nothing ultimately "new" about these abuses; rather, traditions have been repackaged in new forms as "central to a new constitution and configuration of gender" (Adkins, 1999, p.136; Henry & Powell, 2015, p.761, Stoleru, 2014, p.96)

Although the online world has enabled traditional gendered harms and crimes to be enacted in new ways, it would be problematic to overlook the substantive distinctions between offline and online gendered harassment and violence. Due to the unique way in which the Internet allows for individuals to communicate, types of harm and their severity towards victims can be more severe than if the behaviors were perpetrated offline. This is due to three characteristics of the Internet: anonymity, cyber mobs, and the perpetuity of harm (Henry & Powell, 2015, p.763-764).

Anonymity. Anonymity online, although hailed as one of the Internet's most important virtues, can bring out the worst behavior in users that exaggerate the effects of OGHV. The

[3] In the same study, 44% of men claimed to have been harassed online. That the majority of this harassment constituted being called offensive names, being purposefully embarrassed, and physically threatened rather than stalked and sexually harassed. The disparity between the two genders experiences of these behaviors was minimal, with differences of 1%, 2%, and 3% respectively.

Internet provides two kinds of anonymity. The first, "identity anonymity", is the "ability to create information and publish it anonymously or under a pseudonym" (Zharkovsky, 2010, p.215). Most perpetrators of OGHV utilize this kind of anonymity: 26% of online harassment and violence victims claim that their attackers were anonymous, and when taken together with those abused by strangers, over 50% of victims do not know the real identity of their harasser (Duggan et al., 2014, p.26). The second form of anonymity, "access anonymity", allows users to retrieve information on other individuals anonymously (Zharkovsky, 2010, p.215). This implies that content creators have little control over who can access their content, and thus open themselves up to abuse from those who misuse such information. Anonymity of this kind can be seen in cases of cyberstalking where anonymous users gain access to an individual's private information and use it to terrorize the victim.

The two anonymities exaggerate the effect of online harm in a way not possible offline. First, identity anonymity is integral to the "Online Disinhibition Effect" (Zharkovsky, 2010, p.215-216) where individuals become more vitriolic online due to being uninhibited by social cues and norms. In cyberspace, the Online Disinhibition Effect causes users to "behave less defensively and more naturally"; that is, factors in cyberspace such as "lack of eye contact, easy escape, and neutralization of status" influence people to act more destructively due to the belief that their anonymity shields them from external sanctions (Barak, 2005, p.82). Perpetrators of offline harassment and abuse need to be within the same physical proximity to their victim, prompting reactions to social cues such as eye-contact (which can lead to empathy), concerns over social image and, more importantly, the threat of external punishment when their identity can be tied to their actions. When not tied down by these social constraints, it is more likely that individuals will engage in socially inappropriate behaviors in more severe forms and over longer

periods of time. Second, if victims do not know who is posting content about them, they cannot gauge the level of threat posed (Zharkovsky, 2010, p.215-216). Without the knowledge of who is posing the threat, where they are geographically, and how serious the threat is, anonymity causes terror in victims whether or not they are in immediate physical danger. Due to this lack of information, both types of anonymity deprive law enforcement of necessary information needed to arrest and prosecute the most dangerous offenders.

Cyber Mobs. Anonymity and the Online Disinhibition Effect are also key features in the most powerful forms of collective behavior (Postmes & Spears, 2002, p.1075) which, when enacted online, play heavily into another unique feature of cyberspace: cyber mobs. Cyber mobs, the joining together of online users—usually anonymously—to humiliate, manipulate, and attack a specific target (Citron, 2008, p.68-69) has become a new norm for OGHV victims. The lack of temporal and spatial restraints on the Internet allows for users to communicate and band together, which can lead to the formation of hate groups that would have difficulty forming and functioning offline. Online, group dynamics coupled with anonymity influences the behaviors of its members in a condition social psychologists call *deindividuation*: the loss of a person's sense of individuality and personal responsibility. When in groups, individuals tend to lose some of their own self-awareness and self-restraint, and thus will do things they otherwise would not as they feel less responsible for their individual actions (Postmes & Spears, 2002, p.1075). In many cases, deindividuation and online platforms create a feeling of closeness among like-minded individuals and could lead to group members reinforcing negative views and behaviors (Barak, 2005, p.82; Citron, 2008, p.81; Postmes & Spears, 2002, p.1075). In other words, the more an individual sees others within their group enacting OGHV, the more likely they too will engage in those behaviors. An example of this would be “cruelty competitions” where users escalate in

their negative behavior in a need to feel like a member of the group by one-upping the previous "high-fived" abusive comment (Citron, 2014, p.65).

Fighting against cyber mobs is extensively more difficult than opposing a single offline abuser. When an altercation is between an individual and a group of hundreds or even thousands, it is near impossible to shield oneself from all forms of attack. Cyber mobs can coordinate attacks that shut down victims' websites, overload their social media profiles, and even contact employers or police with false charges against targets. Protecting against multiple users who find and distribute victims' personal and private information is also hard to defend against as they not only fail to know who violated their privacy, but also have no control over how the mob may now abuse the information. Merely controlling the flood of negative, harassing, and violent comments from cyber mobs can take time and an emotional toll on victims as they wade through thousands of threatening messages—all the while not knowing which are serious. The size of the cyber mob can also hinder identification of individuals, making it harder for authorities to locate them and charge them with a crime. Even if some individuals are identified and brought to court, this in no way means that others within the group will stop the behavior. In some cases, victims who take legal action against their abusers may actually encourage more severe retaliation from the anonymous mob.

Perpetuity of Harm. The perpetuity of Internet content in OGHV cases magnifies and prolongs victims' injuries. The Internet is a force multiplier as it empowers users to reach large groups of people quickly, allowing salacious and abusive content to spread to an audience of thousands in mere minutes (Zharkovsky, 2010, p.217). Not constrained by physical or temporal barriers, the content can be viewed across the world at any time, soliciting the participation of international citizens in the abuse. Once the material is online, it is difficult to contain or

permanently delete. Content in cyberspace has no natural lifespan as users are able to continuously copy, repost or store the abusive text and images, making it near impossible for victims to find and request its removal on all hosting sites. The online abuse can even become attached to the victim's offline identity through excessively linking and using the victim's name or social media profile within the abusive content. Thus, when entering the victims name in a search engine, results will lead to the negative opinions, harassment, and threats made towards the individual (Citron, 2014, p.67). This harmful online presence can follow the victim years after the initial incident, and impact their social and economic lives. Potential employers for example, may refuse to hire an individual based on their online history. Common reasons cited for not interviewing and hiring applicants have included "concerns about their 'lifestyle', 'inappropriate' online comments, and 'unsuitable' photographs, videos, and information about them (Citron & Franks, 2014, p.352). Employers can also bar victims from employment for fear of the abuse turning towards to the company. Such injuries greatly differ from harassment and violence committed offline where harm can rarely reach many people, and increased efforts to spread the injury "offer diminishing returns" (Zharkovsky, 2010 p.195).

Trivialization of OGHV

If OGHV resembles that of offline gendered harms, why has there been such slow progress in expanding and bringing forth laws that protect victims in the digital medium? In the present, as in the past, prevailing social attitudes towards OGHV against women have shown dismissal, mockery, and trivialization. In part, such dismissal against this new form of delivering gendered harms may hint at underlying gender stereotypes that have yet to disappear from society, while also revealing a lack of understanding of the connectedness between offline space and cyberspace. Nevertheless, it is important to understand current resistance to acknowledging

OGHV as a form of harm so as to dispel mythic assumptions and create adequate protections for victims through both social and legal changes.

First, commentators, law enforcement, and courts have equated OGHV to harmless juvenile antics which warrant little to no response from either victims or authorities. Due to the Internet's facilitation of easy access to strangers, commentators have argued that abuse online has proliferated to the point of meaninglessness, calling it a distasteful but altogether harmless norm of the Internet. Abuse online has been purported to be the work of "*trolls*", bored Internet users hoping to get a laugh by riling up other users. Victims are told not to fuss about their online abuse because it is, as writer Jay Geiger argues, "a bunch of stupid kids saying stupid things" who "will probably cry in front of their mom when they get caught" (Citron, 2014, p.75). Jim Pagels, a sports media and business writer for *Forbes*, in his 2013 *Slate* article wrote; "The stories often give the impression that this is some kind of shocking event for which we should pity the 'victims', but anyone who's spent 10 minutes online knows that these assertions are entirely toothless" (Pagels, 2013, para.3).

Another trivialization of OGHV is the response that targeted individuals have the ability to protect themselves without the need for law enforcement and judicial intervention. A common suggestion to victims is to simply ignore the abuse, prompting the perpetrator to grow bored and leave. Many have advised leaving the online forum or getting off the Internet altogether. Law enforcement officers have even refused to pursue cyber harassment complaints on the grounds that women can "just turn off their computers." Such instruction is not limited to a specific form of OGHV; communications ranging from sexist comments to outright threats of rape and violence have been met with similar responses. One example is the incident involving Catherine Mayer, a journalist at *TIME*, who received a threatening tweet stating; "A BOMB HAS BEEN

PLACED OUTSIDE YOUR HOME. IT WILL GO OFF AT EXACTLY 10:47 PM ON A TIMER AND TRIGGER DESTROYING EVERYTHING." When she reported the threat to the police, she was advised to unplug. In an interview with *Pacific Standard*, Mayer recalled how the officers "were unanimous in advising me to take a break from Twitter…assuming, as many people do, that Twitter is at best a time wasting narcotic" (Hess, 2014, para.25).

It has also been asserted that women can take a more active approach to combating their abusers through counter-speech. As many believe that most perpetrators of OGHV are merely trying to rile up the emotions of their target for fun, it stands to reason that confronting them—whether online or offline—will quickly shame them into leaving. As many victims have a devoted audience on their blogs and social media accounts, commentators also suggest that victims could rally their supporters to create a net of protection while simultaneously shaming the offender into silence: essentially using trolling behavior against the "troll" rather than "playing the victim". Others have claimed that OGHV is a cause for celebration for women, and a chance to show their power and influence rather than act as victims. Hanna Rosin, an editor at *Slate*, argued that "it shows just how far we've come. Many women on the Internet are in positions of influence, widely published and widely read; if they sniff out misogyny, I have no doubt they will gleefully skewer the responsible sexist in one of many available online outlets, and get results" (Hess, 2014, para.10).

There are also those who defend the allowance of OGHV because of the medium, citing the "wild west norms" of the Net (Citron, 2009, p.400). Commentators have suggested that abusive content is merely a part of the territory when it comes to the Internet—a unique characteristic that people "allegedly assume by using networked tools" (Citron, 2014, p.79). Some have even argued that the Internet is not necessarily different than offline communication

in terms of its incivility. As Jen Doll explained in her *The Wire* article on "Twitter Death Threats"; "Is it any more uncivil than anywhere else…? The Internet hardly created hate, or hate-speak, or bullying. Further, do we only increase the levels of that incivility by freaking out about what a bunch of random people are raging about behind the protection, and often anonymity, of Twitter?" (Doll, 2012, para.5). Many Internet users have already internalized this unspoken lawlessness of the Internet and have acted accordingly. For example, one Pew interviewee stated, "it is a general characteristic of the medium and environs … It feels like bottom-feeders are the norm online...." (Duggan et al., 2014, p.29).

Others have argued that these "wild west norms" are deeply tied to the American value of protecting free speech. Commentators argue that while a portion of online abuse may be offensive and distasteful, free speech rights extend to the Internet and regulating, deleting, or denying the allowance of such speech would be a violation of the First Amendment—the bedrock principal of which is that "the government may not [censor] the expression of an idea simply because society finds the idea itself offensive or distasteful" (Citron & Franks, 2014, p.374). Such a basis was established when the Supreme Court famously declared in *New York Times Co. v. Sullivan (1964)*, that our society has a "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open". Thus, hateful and deeply offensive words enjoy presumptive constitutional protection (Citron & Franks, 2014, p.374-375). Those who believe in this "wild west" of free speech argue that attempts to crush "trolling by men" are akin to infringing upon First Amendment rights. *The Telegraph's* Brendan O'Neill remarked:

> "Anyone who cares about freedom of speech should sit up and take notice when campaigners start talking about words and violence in the same breath, because to accept

> the idea that words are as damaging as violent actions is implicitly to invite the policing and curbing of speech by the powers that be. After all, if speech itself is a kind of violence…then why shouldn't internet trolls and foul-mouthed loners be treated as seriously as the bloke who commits [grievous bodily harm]?" (O'Neill, 2011, para.3).

O'Neill, like many other male bloggers and writers, also claimed that such abusive speech is endured by everyone, not just women; "If I had a penny for every time I was crudely insulted on the Internet, labelled a prick, a toad, a shit, a moron, a wide-eyed member of a crazy communist cult, I'd be relatively well-off. For better or worse, crudeness is part of the Internet experience, and if you don't like it you can always read *The Lady* instead" (O'Neill, 2011, para.2). Women, therefore, should not complain if the abuse turns in their direction. The belief that there will always be a dark part of the Internet pervades social thought, and the argument that prohibiting such abuse would infringe on America's most cherished value has caused many to simply shoulder the abuse as "natural" to the space.

Such excuses for inaction should sound familiar as they directly echo that of the past: 1) such harms are not to be taken seriously, 2) women have the ability to avoid the injury themselves, and 3) such behaviors are natural and protected. Modern trivializations have much in common with past suggestions that workplace sexual harassment was mere teasing, and that women could easily leave their violent domestic partners or workplace instead of complaining. Such assertions presume that online damage remains suspended in cyberspace with no effect on women's offline lives, completely disregarding the proliferation and severity of the abuse due to anonymity, cyber mobs, and its online permanence. There are few times when threats of rape and death cannot be taken seriously, and usually overpower emotional bandwidth and take away time and money from the victim (Hess, 2014, para.12). In a cyber mob of anonymous attackers, to

simply “unplug” from the Internet not only deprives a victim of a public resource, but isolates her from an extension of the offline world. While men such as O’Neill claim to also encounter the negatives of the “wild west norms”, few of the comments thrown at males focus on threatening gendered harms such as violent sexual assault and rape.

Due to anonymity, cyber mobs, the perpetuity of online content, and the trivialization of online gendered harms, OGHV behaviors are hard to mitigate and control. Without proper intervention, the prolonged severity causes irreversible harm. While some claim that current laws against harassment and violence already cover prosecuting such behaviors, many of the laws do not encompass how courts should respond when injuries occur across an online medium where there is no concrete concept of space and time. Can someone be sexually harassed through mere images and text, as opposed to the physical harassment once enacted in the workplace? Do aggressive comments online constitute as actual threats when the perpetrator may live thousands of miles from the intended victim? These are the questions that judges and courts have been asking and, due to the changing state and environment of the medium, have had a hard time cementing into law. Victims therefore have scattered and flimsy legal protections that may cover damages done to them in physical space, but ignore the very real and serious harms done to them in cyberspace. In sum:

1. OGHV is the same kind of gendered harm committed in offline spaces
2. The use of the Internet and its unique aspects of communicating these harms exaggerates and prolongs the negative effects to victims in a way unlike that of offline spaces
3. The trivialization of the current harms inflicted upon women from online content not only echoes the dissent against sexual harassment, domestic violence and stalking

laws from the 1970s to 1990s, but has also hindered the acknowledgement of the need for the development of laws that adequately address the issue

4. Because of the new methods and severity of committing gendered harms, many current laws are outdated and inadequate in addressing the problem

This study does not suggest that all distasteful gendered communications online should be unlawful. Much like in offline spaces, individuals are allowed to express their beliefs, including those that are offensive to other groups, without fear of censorship. However, as the Internet becomes more of a staple in human life, the ability for women to participate online and the legal protections afforded to them against OGHV will shape not only future communications, but also influence the very makeup of who and what is available online. To guide this in a positive way, the specific OGHV behaviors outlined within the next section must be recognized for their harms, requiring the need for stricter legal regulations. The following section will thus describe these behaviors by giving them concrete definitions to make them linguistically "real" and, through the use of statistics and illustrations, show why they are serious threats to individuals.

II. Forms of Online Gendered Harassment and Violence

Currently, there are no universal terms with corresponding sets of definitions to describe OGHV behaviors. Scholarly discussions surrounding different forms of OGHV have become muddled with confusing overlaps such as age, severity, and specific actions attributed to the behaviors. Ultimately, such overlaps thwart clear analysis and the creation of successful solutions. In response, this study will attempt to clearly define each behavior and its specific actions and harms. Such clarification is necessary for creating successful solutions for both the

public and legislators. The specific behaviors are discussed under three OGHV categories: cyberbullying, online sexual harassment, and cyberstalking.

Cyberbullying

Past research on cyberbullying has abounded within the last few years, yet researchers have yet to come to a consensus on its exact definition and constructs. With influence from multiple studies descriptions of the behavior, this study classifies cyberbullying as follows: the repeated transmission of any electronic textual, visual, written, or oral communication to coerce, abuse, torment, or intimidate a person under the age of eighteen by another underage individual. The constructs of cyberbullying include malicious intent, violence, repetition, and power differentiation (Bamford, 2004, p.1; Beran & Li, 2007, p.17; Lightburn, 2009, p.4; Patchin & Hinduja, 2006, p.152; Shariff & Gouin, 2006, p.3, Ybarra & Mitchell, 2004, p.1308). Cyberbullying comprises a wide range of behaviors, including but not limited to: "flaming", "denigration", "masquerade", "outings", and "exclusion" (Bamford, 2004, p.2-3; Beran & Li, 2007, p.17; Lightburn, 2009, p.9; Standing Senate Committee on Human Rights, 2012, p.12). Rather than consider cyberbullying as a separate phenomenon, this study proposes that students are merely expanding at-school bullying tactics to include online formats.

Since the introduction of personal computers and the Internet, adolescents and children have been introduced to technology at an early age, the affordability and development of which have made it easy for them to gain mastery. Young people now have access to many "languages" of communication and multiple modes of delivering information, such as frequently combining text, voice, graphics, video and gaming genres, establishing communities, and adapting technology to their needs (Bamford, 2004, p.3). This mastery has allowed adolescents to engage in forms of abuse that they might otherwise not have committed in physical spaces under

parental and administrative watchfulness. Much like the other forms of OGHV, this is due to the unique aspects of Internet communication: anonymity, cyber mobs, and the perpetuity of harm.

A majority of cyberbullying is anonymous as perpetrators shield themselves behind screen names. This lack of accountability for harmful actions can have a variety of impacts. First, anonymity allows anyone to become a bully. Not constrained by appearance and build, cyberbullies can be physically weaker than their victims, a notable difference from traditional face-to-face bullying where bullies used physical intimidation or force to exert control over their victim. This also differs from offline bullies who—though physically weaker—used numbers as a form of social and physical control, as cyberbullies can now attain power over the victim singlehandedly. Further, bullies are emboldened using online communications to carry out their abusive agenda as it "takes less energy and fortitude to express hurtful comments using a keyboard or keypad than using one's voice" (Patchin & Hinduja, 2006, p.154). As anonymity prevents cyberbullies from coming "face-to-face" with their victims, they avoid contextual social cues such as body language, tone of voice, and facial expressions (Bamford, 2004, p.2) that offline would restrain individuals from inflicting harm on others. Without seeing the repercussions of their actions in real-time, anonymity makes it easier for the worst forms of aggression to take place at more frequent and severe levels, such as harassment, sexual humiliation, and threats of violence.

The widespread availability of electronic devices allows for no lack of participants to cyberbully, thus providing a seemingly endless pool of bullying candidates (Patchin & Hinduja, 2006, p.156). While face-to-face offline bullying victims eventually forget the negative things said against them and move on, cyberbullying is concrete and, once transmitted, may be impossible to destroy as the text, images, and videos are accessed, reread and replayed

repeatedly (Campbell, 2005, p.3, Lightburn, 2009, p.12). This prolongs the victim's pain for two reasons: first, these words can feel more "real" than spoken words (Campbell, 2005, p.3) and second, the longer the content persists online the more bystanders join in the abuse, creating an intensified power imbalance between victims and perpetrators. Research on general bullying has found that 30% of onlookers and bystanders support perpetrators rather than victims, but online this percentage can be exponentially larger as classmates and other individuals who may not engage in the bullying at school can hide behind the technology to help inflict serious harm (Shariff & Gouin, 2006, p.3). Further, the fact that at least 93% of adolescents have a computer or have access to one at home (Madden, Lenhart, Duggan, Cortesi, & Gasser, 2001, p.2) indicates that cyberbullying is a more intrusive form of bullying as the abuse follows victims into what was once a safe and private abode. This feature of cyberbullying unquestionably increases the stress and negative consequences for the victim as the bullying becomes perpetual.

While cyberbullying is already considered by many a societal ill, this study goes further in posing that cyberbullying as a whole should also be considered a form of OGHV. Although both sexes engage in and experience cyberbullying, a majority of research has shown that girls appear to be the primary targets in cyber space, and that gender and sexual harassment bullying are the most prevalent forms of cyberbullying among adolescents (Lightburn, 2009, p.14; Shariff & Gouin, 2006, p.4). According to a Pew Research Center report in 2007, girls were more likely than boys to say that they had experienced cyberbullying–38% of girls online reported being bullied, compared with 26% of boys. Older girls in particular were also more likely to report being bullied than any other age and gender group, with 41% of girls ages 15 to 17 reporting these experiences (Lenhart, 2007, p.2). With the rapid increase in use of online communication technologies within the last few years, it is likely that this percentage has also increased.

Research has also shown that not only are females the primary targets of cyberbullying, they can also be the primary perpetrators. Girls tend to use indirect forms of aggression against each other, hence in cyberbullying cases girls spend considerable time breaking confidences and spreading rumors, criticizing physical appearance or personality, and using code names to plot against and ostracize other girls (Owens, Shute & Slee, 2000, p.74-82; Lightburn, 2009, p.32). One plausible explanation might be that girls, who may be more submissive in face-to-face communications, may not feel so constrained online. Their assertive online communication skills thus lead to online harassment (Shariff & Gouin, 2006, p.6-7).

The cases of Nicole Edgington and Lauren Newby are prime examples of gendered cyberbullying. In 2010 when she was a high school senior, Edgington became the victim of a cyberbullying campaign when, on the night of her seventeenth birthday, she began receiving texts calling her a "whore", "slut" and "scared snitch". Horrified, she later learned that there was a secret plan to ambush her and slam her head into cement (Edgington, 2012, para.1-2). While the physical attack was avoided, Edgington became the target of cyberbullying through the use of texts and Facebook. In her own article published in *Choices*, Edgington related how she "received hundreds of threatening texts and messages" and "was terrified of the threats…" (Edgington, 2012, para.5). The attacks followed her both at school and at home as any time she checked her phone or opened her Facebook page she was met with abusive comments, accusations, and threats. Although able to narrow down her attackers to a group of 50 students, the cyberbullying ruined Edgington's social life as she withdrew from the Internet and her peers to escape the abuse.

Lauren Newby's cyberbullying was even more severe, stemming from a thread on a message board by a former student of Newby's school. According to Amy Benfer's report in

Salon Magazine (2001), the thread was called "Lauren is a fat cow MOO BITCH" where, among other things, the anonymous poster, who identified themselves as "MOO BITCH," made fun of Newby for her weight and her bout with multiple sclerosis ("I guess I'll have to wait until you kill yourself which I hope is not long from now, or I'll have to wait until your disease [M.S.] kills you") (Benfer, 2001, para.9). The message board even included an entire page of the words "Die bitch queen!" repeated hundreds of times. The increased cyberbullying online quickly escalated offline. Newby's car was egged, "MOO BITCH" was scrawled in shaving cream on the sidewalk in front of her house, and a bottle filled with acid was thrown at her front door. Newby's mother, who opened the door, suffered minor acid burns, and the arson department was called in to investigate (Benfer, 2001, para.11). These cases are not unique, and for many have escalate to life-threatening. 13-year-old Megan Meier and Hope Sitwell, 15-year-old Amanda Todd, and 18-year-old Jessica Logan—to name but a few—all experienced some form of cyberbullying which drove them to commit suicide.

As seen in these cases, cyberbullying is a problem to the extent that it produces harm towards the victim. Social acceptance is crucially important to a youth's identity and self-esteem, and cyberbullying can capably and perhaps permanently wreak psychological, emotional, and social havoc as "internalizing cyberbullying messages include anxiety, loneliness, sadness, over-compliance, and insecurity" (Beran & Li, 2007, p.19). Past research has found that girls were more likely to have both depressive symptoms and suicidal thoughts when cyberbullied, and girls also reported significantly higher levels of social anxiety than boys due to the collapse of their trust in peer relations (Lightburn, 2009, p.30). Cyberbullying through pictures or video clips was found to be the most offensive, and rated as having the most psychological impact on victims (Ybarra, Mitchell, Wolak & Finkelhor, 2007, p.1176). Of those who reported distress, 44%

reported repeated harassment (Lightburn, 2009, p.29). Age was also a factor in how distress was felt, with younger victims 20% more likely to report emotional distress compared to 8% for pre-adolescent youth.

Significantly, although cyberbullying begins anonymously in the virtual environment, it greatly impacts learning and peer relationships in the physical environment. Fear of unknown perpetrators among classmates and bullying that continues at school can be psychologically devastating for victims. It is also socially detrimental to *all* students, distracting them from schoolwork by creating unwelcome physical school environments where equal opportunities to learn are greatly reduced (Shariff & Gouin, 2006, p.3). With regard to public embarrassment, life in cyberspace is often intertwined with offline life as kids discuss what happened at school online, and vice versa. There is no clean separation between the two realms, and so instances of cyberbullying make their way around the interested social circles "like wildfire" (Patchin & Hinduja, 2006, p.155). Such psychological and physical disruptions, when experienced among members of this impressionable and often volatile population can, at worst, result in "violence, injury, death, and even later criminality for both the initiator and recipient of bullying" (Patchin & Hinduja, 2006, p.149).

Online Sexual Harassment

Gendered harassment online has become the new norm for many females in cyberspace. Constituting unwelcomed verbal and pictorial interactions that insult and threaten individuals due to their gender, the many forms of gendered harassment online have three core features: 1) it's victims belong to historically subordinate groups (i.e. females), 2) the harassment is aimed at particular individuals personally and by name, and 3) the graphic, vicious and public abuse invokes the targeted individual's gender in threatening and degrading ways that interfere with

individual's livelihoods and education (Citron, 2009, p.378; Franks, 2012, p.678). Broadly, gendered harassment online ranges from telling chauvinistic jokes, to sending unwanted sexual messages and threats (Barak, 2005, p.78). Though gendered harassment is negative and disrespectful, not all of its forms should be considered illegal; the First Amendment protects and encourages the right to express disagreement with an idea or person even if it is unfavorable towards a certain group (Markey, 2013, P.4). However, the most damaging and threatening form of online gendered harassment should not be lumped into these protections: online *sexual* harassment. For the purposes of this study, online sexual harassment is defined as unwelcomed verbal or graphic conduct of a sexual nature that creates a hostile environment online. Like offline sexual harassment, online sexual harassment signals to women that they are "either not welcome in a given space and/or that they will only be tolerated in that space under certain conditions of humiliation and 'sexualization'" (Franks, 2012, p.674). This study argues that, like street and workplace sexual harassment, online sexual harassment is a form of social control that attempts to intimidate and restrict female use of public space, and thus is a form of gender discrimination and violence.

Drawing from Barak's (2005) outline of sexual harassment in cyberspace, this study divides online sexual harassment into two categories: verbal and graphic.

Verbal online sexual harassment. Verbal online sexual harassment appears in the form of offensive sexual messages actively initiated by one or more perpetrators towards a victim (Barak, 2005, p.78-79). This includes threats of sexual violence and sexual coercion when they are neither invited nor consented to by the recipient.

Threats of sexual violence. Threats of sexual violence often refer to sexual assault, mutilation, rape, and death, reduce the target to a sexual object, and include the use of "humiliating comments that reinforce gender-constructed stereotypes" (Citron, 2009, p.380). Comments can be varied, but all are derogatory and threatening:

> "if you were my wife i would beat you" (Royse, 2008, para. 3);
>
> "I wouldn't fuck you. I would fuck the shit outcha. Morning, noon and night. Till ya black and blue" (Lee, 2015, para.1);
>
> "you are clearly retarded, i hope someone shoots then rapes you" (Royse, 2008, para.3);
>
> "Better watch your back on the streets whore…Be a pity if you turned up in the gutter where you belong, with a machete shoved in that self-righteous little cunt of yours" (Citron, 2014, p.75)

Such comments utilize the target's gender to make gender-specific threats that reduce women to victims based on their biology and exert power over their bodies. Fueled by anonymity and cruelty competitions, cyber mobs often form and create hostile environments for the target, as well as other women reading the sexualized comments.

One example is the case of Caroline Criado-Perez, a journalist and feminist campaigner who led the charge to get more female faces on England's currency in 2013.While campaigning, Criado-Perez received hostile messages ("Get back to the kitchen", "shut up", "fuck off"), though the content was relatively benign (Hattenstone, 2013, para.5). Following her victory in helping to get famous British author Jane Austen on the back of a tenner however, Criado-Perez became the victim of a firestorm of Twitter messages threatening sexual abuse, rape, and death. In an interview with *The Guardian*, Criado-Perez recounted the kinds of threats she received on a

daily, and sometimes hourly, basis:

> "… someone was talking about giving me a good smashing up the arse…Somebody said: 'All aboard the rape train.' Some guy tweeted another guy asking if he wanted to join in raping me… Then there were the death threats. One was from a really bright guy who said: 'I've just got released from prison. I'd do a lot worse than rape you. I've just got out of prison and would happily do more time to see you berried [sic]. #10feetunder. Another said "I will find you, and you don't want to know what I will do when I do. You're pathetic. Kill yourself. Before I do. #Godie" (Hattenstone, 2013, para.6).

At the height of the abuse, Criado-Perez reported receiving 50 rape threats in a single hour (Brandom, 2013, para.1). Those who showed support for Criado-Perez also received death and rape threats, such as Labor MP Stella Creasy: "You better watch your back....Im gonna rape your ass at 8pm and put the video all over the Internet," read one. Another said: "If I meet you in an alley you will definitely get fucked" (Jones, 2013, para.4-5). Of the 86 different Twitter accounts directing abuse towards Criado-Perez, only two were found and charged with a crime.

Online sexual coercion/ "sextortion". A midway point between verbal and graphic online sexual harassment and abuse, online sexual coercion, or "sextortion" as it has recently been coined, entails the use of various means available online to elicit sexual cooperation by putting some kind of pressure on a victim (Barak, 2005, p.80). Although the use of physical force is impossible online, victims might perceive threats against themselves or their friends and family just as realistic on the Internet as if in face-to-face situations (Barak, 2005, p.80). Usually, online sexual coercion occurs due to an abuser's possession of sexually explicit images of their target. Offenders will either trick individuals into taking and sending sexually explicit content of themselves or, in some cases, hack the target's computer to find compromising material to use as

blackmail. The abuser will threaten to send it to friends, family, schools and employers unless the individual complies with their demands, usually sexual in nature.

The case of Jared James Abrahams, a 19-year-old computer science student from Temecula, California exemplified such behavior. In 2013, Abrahams used malicious software to control female students' computer webcams and take nude photographs or videos. He then sent emails to the victims threatening to publish the photos or otherwise harm their reputations unless they sent him more explicit material (Blankstein, 2013, para.2; Botelho, 2013, para.1). 18-year-old Cassidy Wolf was one of his victims, and the first to bring her abuse to the attention of authorities. Wolf had received a Facebook alert that someone had attempted to change her password, and noticed that her Twitter avatar had been changed to a half-nude picture of herself. She later received a message with other nudes attached from Abrahams, explaining; "Either you do one of the things listed below or I upload these pics and a lot more (I have a LOT more and those are better quality) on all your accounts for everybody to see and your dream of being a model will be transformed into a pornstar (sic)" (Blankstein, 2013, para.5; Botelho, 2013, para.7-9). After police investigated and arrested Abrahams, he was also linked to at least eight other "sextortion" cases of young women, some of whom were from as far away as Moldova and underage (Botelho, 2013, para.13).

Graphic online sexual harassment. The second form of online sexual harassment, known as graphic online sexual harassment, involves the intentional sending of erotic and pornographic images through either individual online communication channels or posting them on online forums (Barak, 2005, p.79). Such content involves digital voyeurism or "creepshots", doctored photos of women in a sexual manner, and revenge pornography.

Digital voyeurism/ "creepshots". Broadly, digital voyeurism, or "creepshots", are instances where individuals surreptitiously take photos or videos of women's private areas for the purpose of sexual gratification. The pictures usually focus on the breasts, butts, and crotches of women, with the latter usually taken by putting the camera underneath or even up a woman's skirt. "Creepshots" differ from revenge pornography in that, while the focus of the image may be a sexualized part of a woman's body, the woman is still clothed, obstructing the view of the full genitalia. In some cases, the act of taking the image without the victim's knowledge, and the subsequent violation of their privacy and agency, is what provides the sexual gratification (Cochrane, 2012, para.3). "Creepshots" act as the digital version of offline voyeurism with one key difference: the possession of photographic "souvenirs". Unlike offline voyeurism, where the individual merely watches the target without their knowledge for a limited period of time, "creepshots" allow for the target to be perpetually violated by both the owner of the images and those with whom it is shared. When distributed on digital formats, this lends the target to be the victim of thousands of perpetrators and, due to the longevity and permanence of Internet content, remain a victim for years.

To add insult to injury, this behavior is currently legal in many states. According to Valenti (2015); "Legally, men who want to secretly film women's body parts largely don't need permission or consent—not from women, not from teenage girls, not from children…if you're in a public place you have no legal expectation of privacy, not even for your private parts" (para.6). Court decisions have even upheld the legality of the practice. In 2014, a court in Washington, D.C. upheld the right of men to surreptitiously take photos of women's private areas, even if the photos were meant for purposes of sexual gratification, as did a judge in Oregon in 2015 after "a 61-year-old man was caught taking photos up the skirt of a 13-year-old girl" (Valenti, 2015,

para.8). In questioning why there is a market for such pictures, one answer is the "familiar combination of desire and humiliation… a sense that female bodies are public property, fair game – to be claimed, admired and mocked" (Cochrane, 2012, para.5).

The most notable case to date is when "creepshots" gained national attention in 2011 and 2012 after a CNN exposé on the prominent Reddit forum called /r/jailbait. The forum, taking its theme from "jailbait's" definition, posted sexual images of girls under the legal age of consent without their or their families' permission. Users posted sexual "creepshots" of the tween and teenage girls, often in bikinis and skirts, many of which were taken from their Facebook profiles without their consent and "thrown in front of /r/jailbait's 20,000 horny subscribers" (Chen, 2012, para.7). The creator of the forum was a 49-year-old man named Michael Brutsch, known online as "Violentacrez". Not confined to /r/jailbait, "Violentacrez" had created hundreds of sub forums on the user-generated website, such as "Rape bait," "Incest," "Pics of Dead Kids," "Choke a Bitch," and "Rape Jokes" (Fitzpatrick & Griffen, 2012, para.2), all of which included images of woman in sexually degrading ways, the pictures usually taken without the individual's consent. In response to the criticism, the forum featured a welcome message that told female visitors, "When you are in public, you do not have a reasonable expectation of privacy. We kindly ask women to respect our right to admire your bodies and stop complaining" (Markey, 2013, p.12).

Doctored photos and threats of violence. Graphic content such as doctored photos of women in sexually compromising positions can also be a common form of online sexual harassment. Commonly, such images are accompanied by textual threats of harm or even death. For instance, Kathy Sierra, a well-known programmer and game developer who maintained a popular blog on software development became the victim of a cyber mob in 2007. At the time, Sierra was one of the most visible women in tech. She taught the Java programming language at

Sun Microsystems, published books on software design that were top sellers on Amazon, and her blog was on Technorati's top 100. Very little of her work at the time could have been considered controversial (Sandoval, 2013, para.1). After writing on a forum about blog comment moderation however, anonymous individuals attacked Sierra on her blog and two other websites. Commentators on one site suggested she deserved to have her throat slit ("fuck off you boring slut . . . I hope someone slits your throat and cums down your gob") and be suffocated, sexually violated, and hanged (Citron, 2009, p.380; Citron, 2014, p.75; Franks, 2012, p.679; Lithwick, 2007, para.1; Valenti, 2007, para.2). Such comments accompanied doctored photos of Sierra with a noose beside her neck, or screaming while being suffocated by lingerie. Commenter of the pictures posted "the only thing Kathy has to offer me is that noose in her neck size" (Citron, 2009, p.380; Nakashima, 2007, para.10). Andrew "weev" Auernheimer, a well-known provocateur, hacker, and anti-Semite circulated the photos, one of which depicted Sierra's children performing what appear to be sex acts. He also emailed graphic threats to Sierra about violating her with a chainsaw, circulated her home address and social security number online, and made false statements about her being a battered wife and a former prostitute. Not only did Sierra find herself a target for identity theft, but all the people who had threatened to brutally rape and kill her now knew where she lived (Citron, 2009, p.380-381; Sandoval, 2013, para.3). Sierra's experience left her fearful to attend speaking engagements and even to leave her yard (Citron, 2009, p.385). The harassment and threats—with the graphic images considered some of the worst of the abuse—forced Sierra offline, where she did not return to write until 2014.

Revenge pornography. Instances of revenge pornography have been at the forefront of the graphic online sexual harassment that women experience. According to Genn (2014), revenge pornography is a "form of sexual assault involving the unauthorized distribution on the

Internet of intimate photographs and videos of a nude individual posing or engaging in various sexual activities" (p.165). This includes "images originally obtained without consent (e.g., hidden recordings or recordings of sexual assaults) as well as images originally obtained with consent, usually within the context of a private or confidential relationship" (Citron & Franks, 2014, p.346). According to Henry & Powell (2015), while covert filming of sex acts without consent is by no means a new phenomenon, new communication technologies "enable the distribution of sexual images and footage to be shared across vast geographical spaces", creating "a unique medium for social shaming" (p.767). Contrary to offline means where distribution of a person's nude photo could only reach a limited audience, technology has enabled the nudes to be viewed and shared by thousands of people. Also, whereas offline it might be difficult for a viewer of the nude to know who the individual was, online forums allow for the jilted-ex to connect the picture to the depicted individual by making the image appear prominently in a search of the victim's name (Citron & Franks, 2014, p.350). Online methods have provided a staggering means of amplifying the extent to which individuals can access and spread nonconsensual pornographic content.

The case of Holly Jacobs is arguably the most publicized incident of revenge porn. In 2009, a friend of Jacobs informed her that her Facebook had been hacked, and that the offender had changed her profile picture to a nude photo of herself (Miller, 2013, para.13). Months later, more material of Jacobs appeared on other websites, including a video entitled "Masturbation 201 by Professor Holli Thometz" (Jacobs original name) that was sent to her fellow students at FIU (Miller, 2013, para.18). Problems reemerged for Jacobs years later when, in November of 2011, nude photos of her were posted on the site www.doxed.me., clearly labeled with her identity. Jacobs received a threatening email telling her to reply or face her pictures being

distributed. Three days later, Jacobs pictures were on over 200 websites and had received a myriad of sexually graphic emails ("WOWWWWWWWWW! Couldn't even get through all your hot ass pics babydoll...Blew a load on the mirror self pics… Absolutely incredible ...Thanks!") (Jacobs, 2013, para.9-12). Explicit videos of Jacobs also began circulating the Web. Although Jacobs attempted to save her online image herself after having been turned away by police, within weeks the explicit content was back online and up on 300 more sites (Jacobs, 2013, para. 16-17). Jacobs was forced to change her job and legally change her name.

The dangers of revenge porn are particularly severe to victims' online and offline lives. According to Citron and Franks (2014), in a study of 1,244 individuals, over 50% of victims reported that their naked photos appeared next to their full name and social network profile, and over 20% of victims reported that their e-mail addresses and telephone numbers appeared next to their naked photos (p.351). The distribution of revenge porn, especially when combined with a person's contact information, raises the risk of offline stalking and physical attack by encouraging strangers to confront the victim offline. Many times, fear is warranted as men have called and even arrived at victims' homes demanding sex, with some cases ending in physical assault and rape. Revenge porn specifically has also been cited as belonging to the category of violence that violates legal and social commitments to equality by denying women and girls control over their own bodies and lives—usually as a form of domestic violence(Citron & Franks, 2014, p.351, 353). Frequently, the intimate images are themselves the result of an abuser's coercion of a reluctant partner, and numerous cases involve abusers threatening to disclose the images if victims attempt to leave the relationship. The threats act as a way to keep partners under control, the same as how domestic violence offenders use physical altercations to keep their partners submissive. Despite this violence however, only 27 states have revenge

pornography laws, most of which only classify the behavior as a misdemeanor (Cyber Civil Rights Initiative, "n.d.") Due to the use of sexual content to cause both mental and physical harm towards women, this study classifies revenge pornography as both the most severe form of online sexual harassment and a sex crime.

Previous research has shown that, overall, women are the targets and men the perpetrators of such online sexual harassment and abuse. Mitchell, Finkelhor and Wolak (2001), in a survey of American teenagers, found that 19% of youths, mostly older girls, had experienced at least one sexual solicitation while online in the past year (p.3011). Of those individuals, 3% received aggressive solicitations, and 25% of the solicited individuals reporting they were very or extremely upset or afraid as a result (Finkelhor & Wolak, 2001, p.3013). In 2009, the University of Maryland's Electrical Engineering and Computer Department studied the threat of attacks associated with the chat medium Internet Relay Chat and found that "users with female names received on average 100 'malicious private messages' which the study defined as 'sexually explicit or threatening language' whereas users with male names received only 3.7…" (Citron, 2009, p.379). The study explained that these attacks came from "human chat users who selected their targets, not automated scripts programmed to send attacks to everyone on the channel", and that "male human users specifically targeted female users" (Citron, 2009, p.379). The nonprofit organization Working to Halt Online Abuse ("WHOA"), which compiles statistics about individuals harassed online, found that between 2000 and 2012, 72.5% of victims were female as opposed to 22.5% male victims, while 47.5% of perpetrators were male compared to 30.25% female. In a study conducted by the Cyber Civil Rights Initiative, 90% of those victimized by revenge porn were female (Citron & Franks, 2014, p.353).

By invoking women's sexuality and gender, online sexual harassment and its many forms

are considered major obstacles not only to the free, functional, and joyful use of the Net, but also to women's rights. By causing extreme emotional, economic, and physical harm, online sexual harassment interferes with women's agency, livelihood, identity and well-being. Like all forms of sexual harassment and discrimination, online sexual harassment is not about sex, but about power. Previous research has empirically supported that sexual content and sex is "only a means of satisfying the perpetrator's need for power and domination" (Barak, 2005, p.82). Such harassment has a profound effect on targeted women, discouraging and even forcing them to stop participating online—a practice that, for individuals like Kathy Sierra, may be the source of their livelihood—change jobs, and even change their names (Markey, 2013, p.12). To avoid future abuse, women assume gender-neutral pseudonyms, compromising their female identity online by engaging in stereotypically male conduct and stifling their own female attributes (Citron, 2009, p.374; Gumbus & Meglich, 2013, p.48). This can have a significant price as "hiding one's identity produces feelings of alienation as the person must pretend to be something she is not. It generates feelings of shame. At its most extreme, the impulse to pass or cover can negate a person's identity so completely that she experiences a slow death of 'the psyche, the soul, and the persona'" (Citron, 2009, p.388).

The abuse can also have a physical impact on victim's bodies without the need for physical contact from their harassers. According to Citron and Franks (2014), victims struggle with anxiety, anorexia nervosa, depression, and some suffer panic attacks (p.351). Researchers have found that cyber harassment victims' anxiety grows more severe over time and, according to a study conducted by the Cyber Civil Rights Initiative, over 80% of revenge porn victims experienced severe emotional distress and anxiety, with some women committing suicide (Citron, 2009, p.374; Citron & Franks, 2014, p.351). In some cases, women have even become

more vulnerable to being harassed and attacked offline, a clear indication that such abuse has wide-ranging physical consequences, despite arguments to the contrary.

Cyberstalking

Cyberstalking is considered to be the most dangerous type of cybercrime (Cox, 2016, p.2). However, recognition and delineation of cyberstalking has been slow to come to the forefront of public attention. Currently, there is no singular definition for cyberstalking as it varies among states, different regions of the world, and even academic literature (Ahlgrim, 2015, p.5; Freiberger, 2008, p.8; Fusco, 2014, p.5; Goodno, 2007, p.126). Debate on whether cyberstalking should be considered an extension or variation of offline stalking or an entirely separate action is also a prevalent debate. After examining multiple descriptions of the behavior to distinguish commonalities, this study defines cyberstalking as follows: the repeated pursuit of a person by one or more individuals that involves 1) repeated threats and/or harassment 2) by the use of electronic mail or other computer-based communication that 3) would make a reasonable person afraid or concerned for their safety. This comprises both emotional and behavioral components, where the victim is harmed by constant suffering stemming from fear (Baum & Rose, 2009, p.1; Freiberger, 2008, p.21; Fusco, 2014, p.5; Goodno, 2007, p.128; Strawhun, Adams & Huss, 2013, p.715). Cyberstalking can include technologically surveying or following a target, threats of violence, posting sensitive information online, and technological attacks (Sweeny, 2014, para.8).

In defining cyberstalking, two things must be made clear. First, many times cyberstalking is combined with online sexual harassment. Episodes of sexual harassment can also constitute as cyberstalking when repeated sexualized threats come from a single or group of individuals. Despite the two behaviors close connection, it is important for the sake of designing efficient

laws against the different forms of OGHV that the two be clearly separated through definition. Cyberstalking involves repeated harassment and abuse through technology which does *not* have to be of a sexual nature, whereas online sexual harassment *is* of a sexual nature and *does not* need to be repeated by a single perpetrator. Second, for the purposes of this study, cyberstalking is classified as a related but altogether separate behavior than offline stalking. Although cyberstalking and offline stalking are similar in that they both consist of a desire to control the victim by repeated threatening or harassing behavior (Ajmani, 2011, p.313), it is disparate from offline stalking as it exploits technology to access and spread information about the victims—the magnitude of which would not be possible in offline cases.

Although stalking within the last two decades has become better recognized as harmful criminal behavior, the information revolution and development of the World Wide Web has "increased the arsenal of a stalker" (Spitzberg and Hoobler, 2002, p.72), allowing cyberstalkers to employ new forms of stalking not covered under current legislation. Increased access to other individuals, some of whom stalkers would never have physically come across, has increased the potential for interpersonal and informational surveillance and intrusion, affecting both the online and offline life of the intended victim. Such ease of access for stalkers is also occurring at a time where individuals are providing more information about themselves online. Utilizing websites, as well as more invasive technological attacks, it is now easier than ever for cyberstalkers to follow and abuse their victims, sometimes without even leaving their home. Five key factors make up the most dangerous weapons in a cyberstalking arsenal: instantaneous and repetitious communication, physical separation, anonymity and false identities, third-party stalking, and invasive technological methods (Ahlgrim, 2015, p.9; Freiberger, 2008, p.11; Goodno, 2007, p.127; Shimizu, 2013, p.118).

Instantaneous and repetitious communication. Cyberstalkers can threaten and harass victims instantaneously and with more frequency than offline stalkers due to their almost uninhibited access to information and the victim. Large amounts of information are stored online, blurring the line between what is public and what is private information. Coupled with the Internet's widespread adoption and individual's willingness to provide their personal information, such openness has impacted the "expectations of what privacy is, what is entails, and the degree of privacy that can be expected" (Ahlgrim, 2015, p.4). Both public and private information stored online can be easily accessed either through personal knowledge of the Internet, or through paid online information agencies that gather the information for an individual (Ahlgrim, 2015, p.6-7; Goodno, 2007, p.132). Stalkers can find information about their targets from a number of public sites, such as the target's social media profile, blog, or personal web page. Other identifying information can typically be available through search engines, including "work place details, addresses, telephone numbers and organizations or groups to which an individual may belong" (Roberts, 2008, p.277). This unprecedented divulgence of personal data from potential victims allows for a single perpetrator to access the information with ease while remaining anonymous. (Ahlgrim, 2015, p.4-5; Pittaro, 2007, p.185; Roberts, 2008, p.276). To gain access to more classified data, cyberstalkers can use remote accessing programs that are commercially available (King-Reis, 2008, p.140).

Instantaneous communications between the victim and perpetrator are also facilitated by the Internet as it provides a wide range of opportunities for interactions between individuals who otherwise would not have met. While this is considered a virtue of the Internet, such access also expands the pool of possible victims for a cyberstalker, and has increased cases of stranger cyberstalking (Ahlgrim, 2015, p.5; McGrath & Casey, 2002, p.89; Roberts, 2008, p.277). What

makes this access to individuals so unique from offline stalking is that perpetrators with even limited technological skills and sophistication can engage in cyberstalking and surveillance by merely sifting through chat rooms or looking up images and blogs. According to Ajmani, (2011), the cyberstalker can also easily set up his e-mail account to automatically send intimidating messages repeatedly—potentially thousands of times—to the victim, and that this immediacy of Internet communications can "amplify intimidating language because individuals have less time to reflect upon the effects of their words" (p.315). Such low-effort surveillance is also less likely to be detected than physical surveillance, thus emboldening cyberstalkers to take more abusive action. According to McGrath and Casey (2002), in addition to providing the stalker with more information about the victim, the surveillance and continued access to interacting with their target "may feed voyeuristic fantasies and increase perceptions of power over the victim" (p.84).

Continued access to the victim by the perpetrator also means that victims have continued access to abusive content. Cyberstalking can "easily snowball online as the stalker can create a harassing e-mail, blog, or social media message that the computer systematically and repeatedly sends to the victim thousands upon thousands of times" (Goodno, 2007, p.128-129). Cyberstalkers can also create websites, blogs, and social media accounts for the specific purpose of cyberstalking, on which they post harassing and threatening statements towards their victim—many times mentioning them by name so as to directly link the victim with the abusive content. When copied and shared by the world wide audience, the victim may find it hard to avoid the abuse whenever they go online, which eventually compounds into severe psychological distress.

Physical separation. A major characteristic of cyberstalking is that cyberstalkers can pursue their victims regardless of geographic proximity (Ahlgrim, 2015, p.5-6; Ajmani, 2011, p.316; Freiberger, 2008, p.11; Goodno, 2007, p.129). The Internet has become the fastest and

cheapest form of communication; this efficiency, combined with disinhibition, depersonalization and the omnipresence of the Internet, makes it incredibly easy for cyberstalkers to cause fear and exert control over victims despite not always being physically close (Ahlgrim, 2015, p.4; Ajmani, 2011, p.316; Pittaro, 2007 p.184-185; Roberts, 2008, p.276). While in offline stalking cases there has to be a close proximity between the two individuals, cyberstalkers can be in the next cubicle, across the street, in another state or even in another country. Because there is no physical contact between the cyberstalker and victim—at least while the interaction remains purely online—it is harder for victims to not only identify their abuser, but also locate them for authorities (Pittaro, 2007, p.185). Because cyberstalking may prelude to other dangerous and disturbed behaviors, some of which may end in violence, the inability to discern how likely the ease of access the cyberstalker has to the victim offline can cause considerable emotional and mental distress.

Anonymity and false identities. By either remaining anonymous or creating a false identity online, cyberstalkers make it harder for victims to identify the offender and stop the abuse (Deirmenjian, 1999, p.411). Anonymity creates a shield for the cyberstalker as they can not only avoid culpability for their actions, but also cause fear in their victims. When individuals have no conception of who is threatening them, "it is difficult to evaluate the threat accurately, which may lead to more fear and uneasiness" (Ajmani, 2011, p.314). In fact, cyberstalkers who threaten their victims anonymously can have "an even stronger and more harmful psychological impact on their victims by taking advantage of individuals' simple fear of the unknown" (Ajmani, 2011, p.315). Such power can also embolden cyberstalkers to the point where they may engage in offline stalking (Goodno, 2007, p.130). Further, when the victim does not know the identity of the cyberstalker, law enforcement's ability to investigate and locate the individual is

dramatically reduced. Using technology to their advantage, cyberstalkers use fake social media accounts, anonymous email re-mailers that strip information from messages, anonymous forged emails and more to hide their identity (Ajmani, 2011, p.314; Roberts, 2008, p.278).

Impersonating individuals close to the victim, or even the victim themselves, is also a common form of cyberstalking that would be nearly impossible offline. An offender can ruin a victim's life when posing as them online, whether pretending to be them to friends and family or on online sites. While masquerading as the victim, the cyberstalker can "send lewd e-mails, post inflammatory messages on multiple bulletin boards, and offend hundreds of chat room participants", all of which "affect both a victim's personal life and private life, without them even being aware of the situation caused by the offender" (Ajmani, 2011, p.317; Goodno, 2007, p.131). Additionally, viewers of the posts and receivers of the messages may "respond to the victim with similarly offensive language, threats, or perhaps even criminal activity" (Ajmani, 2011, p.317) which strain victims' relationships with their friends, family, and online communities, isolating them from networks of support. Offline harm can also occur from this appropriation of online identities, especially when combined with online sexual harassment behaviors. Such actions are common in stalking cases involving revenge pornography as abusers pretend to be the victim and solicit (sometimes violent) sex under their name. Unknowing individuals respond to the solicitations and show up at the victim's house, registering the victim's legitimate fear for her life as part of the sexual fantasy described in the online ad (Fusco, 2014, p.6-7). By being unable to tell where messages originated and by whom, it is difficult for victims to deter their abuse and harder for police to apprehend the individuals.

Third party stalking. Perhaps one of the more unique aspects of cyberstalking is that cyberstalkers incite third parties to do their stalking for them. Third party stalking is known as a

type of stalking by proxy, where the perpetrator incites others to knowingly or unknowingly engage in harassing activities on his behalf (Ajmani, 2011, p.318; Freiberger, 2008, p.11; Goodno, 2007, p.132; Roberts, 2008, p.275). Coupled with anonymity and false identities, the cyberstalker can pose as the victim online and post information or solicitations that cause other individuals to send the real victim harassing or threatening messages, or pursue them offline (Ahlgrim, 2015, p.7; Goodno, 2007, p.132; Pittaro, 2007, p.185; Shimizu, 2013, p.119). In regards to asking third parties to knowingly help stalk the victim, a cyberstalker will usually be active on websites and chat groups that tailor to their own interests. By communicating with other individuals who share their interests, the cyberstalkers exchange information on how to harm the victim and encourage each other to take action. For example, if one cyberstalker posts a comment or sends a message regarding their victim, others are likely to respond and take part, leaving the victim with "not just one offender, but multiple offenders attacking, harassing, and threatening them at the same time" (Fusco, 2014, p.8)

Invasive technological methods. Finally, cyberstalkers use of technology to follow, invade, and prevent the victim from participating online acts as the most extreme attempt to exert control over the victim. The technology commonly utilized by cyberstalkers can include email, instant messages, chat rooms, bulletin boards, blogs, Internet sites, social networking, monitoring devices, GPS, cameras, viruses, and other computer programs (Deirmenjian, 1999, p.407; Freiberger, 2008, p.22; King-Ries, 2011, p.137; Roberts, 2008, p.274, WHOA, 2011). Overall, email has been found to be the primary method used by most cyberstalkers as it allows for harassing, threatening, hateful and obscene messages to be sent in a variety of formats (written, audio, visual, pictorial etc.) directly to the victim (Pittaro, 2007, p.186; Roberts, 2008, p.274, WHOA, 2011; WHOA 2012). For more technologically advanced cyberstalkers, email also

allows for the hidden placement of viruses or Trojans in the message without the victim being aware their computer has been compromised (Pittaro, 2007, p.186). Facebook and websites were the second and third most likely places cyberstalking began respectively (WHOA, 2012).

Cyberstalkers who do not want to directly communicate with their victims also have several options that can be pursued. One method at disposal is "Google bombing", or artificially boosting the number of searches for a particular term or phrase so that it appears on "Google Hot Trends" or the search bar's autocomplete (Markey, 2013, p.9-10). "Google bombs" are accomplished through heavy linking using Google's search engine and algorithm. Google's search engine tends to think that the words used in the link to a particular source reflect some of the content of the source. If many people link to an article using a particular phrase, such as a person's name, Google will assume that the name is related to the content of the page, even if that particular phrase isn't used within the page itself. Thus, Internet users through heavy linking can make it so that the first website to appear when searching a woman's name is the one in which she is being constantly harassed and abused. Such actions make it near impossible for the victim to escape their abuse as the vitriolic content follows them wherever they move or whatever jobs they apply for.

The most detrimental cyberstalking behavior however, is the release of victims' private information and inhibiting their use of the Internet. A common cyberstalking tactic is "doxing"[4], the practice of researching, releasing and circulating personally identifiable information about an individual, commonly including a full name, address, phone numbers, email address, and passwords. Depending on how obsessively the cyberstalker pursues the victim's information, he can also release medical and financial histories, lists of schools attended or those of known

[4] From the word "dox", the abbreviation of "documents"

relatives, and social security numbers (Markey, 2013, p.9). While not only an invasion of victims' privacy that puts them at risk for identity theft, doxing also makes victims more vulnerable to third party stalkers and abusers. Cyberstalkers can also employ denial-of-service ("DoS") or distributed denial-of-service ("DDoS") attacks. DoS attacks are attempts to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. DDoS attacks are where there is more than one attack source that targets a victim's website by overloading the number of users attempting to access it (Markey, 2013, p.10). Usually this is done by instigating third party stalkers, thus attacking the site with large numbers of individuals. Attacks can shut down a victim's website or online accounts for days, preventing them from reaching out to their online community and reporting their abuse to gain assistance. All such technology also provides opportunities for cyberstalkers to avoid being personally identified by being difficult to trace (King-Reis, 2011, p.139-140). Though these attacks could be used for other OGHV behaviors, their continued employment against an individual fulfills the requirement of "repeated harassment and threats" to "instill fear" in "a target" that makes up this study's definition of cyberstalking.

The ultimate case: "Gamergate". No other case of cyberstalking has been more publicized than the social media affair known as "Gamergate". In August of 2014, jilted ex-lover Erin Gjoni posted a 9,425-word screed titled "The Zoe Post" on multiple social media sites that featured private details about his relationship with independent game designer Zoe Quinn. After their breakup in early 2014, Gjoni used his expertise as a software engineer to engage in a months-long campaign of cyberstalking, extracting details from Quinn's Facebook history, email, and even their previous texts to track her movements and shadow her conversations. Gjoni

then archived Quinn's private information—ranging from her flirtations, anxieties, professional grudges, and confessions about her family and sex life—on his laptop and cell phone (Jason, 2015, para. 9, 22). Organizing his screed into seven chapters—with titles such as "Damage Control" and "The Cum Collage May Not Be Accurate" to attract a specific readership—Gjoni falsely alleged Quinn had cheated on him five times, and implied she had slept with game reporter Nathan Grayson to get good reviews on her newest game (Jason, 2015, para.25; Stuart, 2014, par.18). Gjoni then posted "The Zoe Report" on 4chan and two other gaming websites that had a history of its users attacking Quinn, believing that "the odds of Quinn's being harassed were 80 percent" (Jason, 2015, para.26).

Within minutes of the post going live, Quinn became the target for hundreds of third-party cyberstalkers and harassers. Someone altered her biography on Wikipedia to read "Died: October 13, 2014", the date of Quinn's next scheduled public appearance, strangers sent Photoshopped images of her covered in semen, and others tweeted abuse (Jason, 2015, para.4, 34-35):

> "Im not only a pedophile, ive raped countless teens, this zoe bitch is my next victim, im coming slut"
>
> "If I ever see you are doing a pannel [sic] at an event I am going to, I will literally kill you. You are lower than shit and deserve to be hurt, maimed, killed, and finally, graced with my piss on your rotting corpse a thousand times over"
>
> "We have to rape Zoe Quinn and take everything from her. We have to ruin her life"

Messages such as "could kill yourself. We don't need cunts like you in this world" preyed on the knowledge that Quinn struggled with depression. Internet users also began to hack and dox her,

releasing her social security number and other private information over the Net (Jason, 2015, para.4; Stuart, 2014, para.19). Third-party cyberstalkers threatened Quinn's father, her current boyfriend, and even her boyfriend's future employer in France until the company rescinded his job offer (Jason, 2015, para.35). In an interview with *Boston Magazine*, Quinn claimed that Gjoni encouraged the cyber mob to cyberstalk her by releasing additional information online, and had taunted her directly over Twitter, claiming; "I am actually doing a lot more than you know in the background" (Jason, 2015, para.41).

The stalking and abuse also spread to other females in the gaming industry. Cyberstalkers began to search for and release troves of women's (and some men's) private information, and coordinated threats for months. According to Jason (2015), a few even "*swatted*" their victims, tricking police dispatchers into sending SWAT teams to raid women's homes (para.43). Brianna Wu, founder of the Boston-based Giant Spacekat, was another target of Gamergate when she was forced to flee her home in Arlington after anonymous cyberstalkers leaked her address. Wu had been receiving dozens of death threats, including a YouTube video depicting a man wearing a skull mask speaking to the camera calling for Wu's death to "bring back the way it used to be in the 1950s [when] there weren't any bitches in video games" (Jason, 2015, para.44). Quinn, Wu, and several other women were forced to flee their homes due to the barrage of threats and the leak of their private information.

Despite the growing concern of cyberstalking from instances such as Gamergate, as a relatively contemporary crime there is little information on its prevalence. According to Ahlgrim (2015), few studies have produced reliable rates of cyberstalking, mostly due to methodological issues (p.7). For example, this study's examination of current literature found that many studies collapsed offline and online stalking incidents into one category, or did not remove rates of

cyberstalking from rates of harassment online. Currently, cyberstalking rates are estimated at anywhere from 1% to 82%. It is also thought that cyberstalking is severely underreported, with possibly only half of all incidents being reported (King-Ries, 2011, p.142). This contributes to a lack of completely reliable prevalence rates being established (Ahlgrim, 2015, p.8).

Although information on cyberstalking's prevalence may be hard to pinpoint, other studies conclusions in regards to cyberstalking being a historically gendered crime are significant. As noted by the Attorney General in 1999; "As with offline stalking, the available evidence…suggests that the majority of cyberstalkers are men and the majority of their victims are women" (King-Reis, 2011, p.137). A study conducted by WHOA in 2002 found that 71% of cyberstalking victims were women (Pittaro, 2007, p.190), and more recently in 2011, WHOA—by *solely* examining cyberstalking—again found that males (40%) cyberstalked more often than females (33.5%)[5]. Smaller studies have also confirmed this as a gendered practice. D'Ovidio and Doyle (2003) examined the characteristics of cyberstalking victims from 171 closed cases investigated by the Computer Investigation and Technology Unit of the New York Police Department: 52% of victims were female as opposed to 35% of victims being male (Roberts, 2008, p.279).

Past research has found serious mental, emotional and physical implications for victims of cyberstalking. Spitzberg and Cupach (2007) identified three levels of stalking repercussions which can be applied to cyberstalking: first, second and third order effects. First order effects are the direct impacts on the victim such as psychological, physical, emotional, or financial costs associated with avoiding or coping with the unwanted pursuit (p.73). First order effects include:

[5] In the same study, 26.5% of cases did not know the gender of the offender

> "impacts on the individual's affective health (fear, anxiety, shame, loss, suicidal ideation, depression, sleep disturbances, impaired psychological well-being) social health (decreased trust, increased alienation and isolation, restricted social activities), resource health (additional security measures, absenteeism from work), cognitive health (maladaptive beliefs, attributions of self-blame, personality adaptation), physical health (physical and sexual violence) or resilience" (Roberts, 2008, p.273-274).

Other physical changes can also occur in the victim, such as abrupt changes in eating patterns and hyper vigilance (Stalking Resource Center, 2012, p.1; Pittaro, 2007, p.191). Second-order effects are the disruptions that occur among the social and institutional networks affiliated with the victim, and third-order effects are unique effects that result among these network members as the unwanted pursuit may begin to affect them directly (p.73). For example, second order effects can include family members spending more time consoling victims, or friends changing their daily behaviors to accommodate the victim's stress. Third order effects, on the other hand, can include those who try to help the victim—such as defending them online or helping to take down negative content—becoming the target for cyberstalking as well.

Escalation of cyberstalking and its harms can also occur should the behavior not be addressed. Due to the obsessive nature of cyberstalking, there "are no guarantees that an online stalker will not, at some stage, transition to stalking their victim(s) offline" (Roberts, 2008, p.279). Cyberstalking situations could evolve into offline stalking where the victim may experience excessive and abusive phone calls, vandalism, threatening or obscene postal mail, and trespassing, and physical assault (Freiberger, 2008, p.29). Some cyberstalkers have even committed murder.

Concluding Remarks about OGHV Behaviors

Cyberbullying, online sexual harassment, and cyberstalking are not only digital forms of sexual harassment and domestic violence, but of discrimination and abuse. By using threatening language, images, and cyber attacks to abuse and exclude females online, perpetrators are denying women autonomy over their own bodies and voices in cyberspace. These effects are not inconsequential; OGHV "damages women as a group and society as a whole by entrenching a gendered hierarchy in cyberspace", the use of repeated demeaning, sexualized comments and rape threats suggesting men's power and superiority over women, and instilling the notion that online spaces are male spaces (Citron, 2009, p.390). Due to the volume and viciousness of attacks on women by men, this suggests that "cyberspace cannot be thought of as a place where, on balance, women and men can participate equally. Rather, it is a place where existing gender inequalities are amplified and entrenched" (Franks, 2011, p.2).

History has shown that such abusive behaviors are not accepted within society, but effective laws must be put in place to ensure that those who would ignore individual's rights are punished. The 1970's to 90's provided laws that guaranteed respect, protection, and equal opportunity for women, which even today are still used to combat incidents of injustice. Just because this abuse is now being enacted online does not mean that these rights have disappeared or stop at the digital border. But there is no justice in laws that allow perpetrators of these crimes avoid prosecution due to their use of the medium, or receive minimum punishments that do little to stop the abusive behavior. As this next section will detail, while current laws may at times act as appropriate barriers and punishments for *offline* gendered crimes, the criminal justice system has yet to develop an effective response to abuser's online actions.

III. Inadequate Laws, Policies, and Prosecution Schemes

There has been nearly nationwide acknowledgement of the role that online communications play in harming others. To the credit of both federal and state governments, this acknowledgement has led to legislators enacting laws to account for at least one form of cyber victimization (Schwartz, 2009, p.416), including those this study has classified as OGHV. For example, a total of 37 states have cyberstalking laws, while 41 have cyber harassment laws (Marwick & Miller, 2014, p.21-22). There are currently a multitude of ways victims can theoretically address their abuse through both civil and criminal law. Tort claims— "a body of law that requires defendants to compensate plaintiffs whose injuries they have wrongfully caused"—provides redress for victims' damaged reputations and emotional well-being through defamation and intentional infliction of emotional distress, to name but a few (Citron, 2014, p.120-121). State and federal criminal law on the other hand punishes stalking, harassment, extortions and credible threats of violence. This includes the The Federal Interstate Stalking Punishment and Prevention Act (18 U.S.C §2261A), the Interstate Communications Act (18 U.S.C. §875*)* and the Telecommunications Harassment Statute (47 U.S.C. §223). These laws specifically stipulate that an "interactive computer service" or "electronic communication service" cannot be used to threaten, abuse, harass, and intimidate another person (Citron, 2014, p.124-125; Cox, 2014, p.3; Sweeny, 2014, para.11; 18 U.S.C §2261A; 18 U.S.C. §875; 47 U.S.C. §223). Using the Internet to solicit strangers to attack or stalk an individual, hack into private accounts, film individual's nude bodies without consent, and abet in identity theft by publishing someone's social security number is also criminalized under the law.

Despite this attempt by legislators to account for the dangers of online victimization, current gaps in policies do not punish the full spectrum of problematic cyber behavior. Current

laws are inconsistent, at times inadequately developed, and may not criminalize all forms of OGHV behavior (Citron, 2014, p.124, Cox, 2014, p.5, Schwartz, 2009, p.409; Shimizu, 2013, p.123). Many of the laws make protecting victims extremely difficult, with some jurisdictions making the legality of OGHV behaviors ambiguous (Ahlgrim, 2015, p.9). Additionally, gaps in police-force education and prosecution pose a barrier for victims as many police agencies don't allocate resources to fighting this type of crime, or are uneducated in how to address it (Jameson, 2008, p.255; Sweeny, 2014, para.19). Often, victims who go to the police are told it's a civil matter, not a criminal one, when there are indeed criminal laws in place to stop the abuse. Moreover, many civil laws are costly and invasive, and unintentionally pose additional barriers for successful prosecution (Cox, 2014, p.5; Sweeny, 2014, para.7). Internet service providers and website administrators may also refuse to help OGHV victims and police, allowing the content to spread unheeded.

Although OGHV occurs online, perpetrators are subject to the same laws and torts as offline abusers. However, as the laws were developed for offline harms, the policies have not been adequately updated to reflect digital platforms of communication. This study identifies gaps in the laws so that reformations can be proposed.

Civil Torts

Civil torts, wrongs that result in an injury or harm that constitute the basis for a claim by the injured party, is one of the most common forms of redress victims of OGHV are told to turn to. In theory, civil torts address the harms done to victims that may not constitute a criminal offense. However, many barriers exist in bringing successful claims exist for victims. In civil tort cases, money can act as an obstacle for victims; unlike criminal cases, claimants take on the full costs of the civil suit, a burden that may be impossible when the victim has already lost her job

due to the online abuse (Cox, 2014, p.5; Sweeny, 2014, para.7). Victims who are able to pay for the civil suits may also be hesitant to prosecute their abuser if the litigation requires their real name, as the possibility of the public seeing the abuse and exacerbating the threatening online behavior may make the victim fear bringing the case to court (Citron, 2014, p.122).

Defamation. One of the first civil remedies that victims of cyberbullying, verbal online sexual harassment and cyberstalking are theoretically able to pursue against their abusers is the tort of defamation. Defamation refers to a statement that injures a third party's reputation. Defamation law attempts to protect against various types of reputational harm, including "reputation as property, as honor, and as dignity" (Jameson, 2008, p.246). As defined by the *New York Times Co. v. Sullivan* (1964) case, in order to succeed in a defamation lawsuit, a plaintiff must meet six elements that comprise a libel claim: (1) a defamatory communication; (2) a false statement of fact; (3) publication of the false message to a third person; (4) identification of the plaintiff; (5) depending on the private or public nature of the plaintiff, fault on the part of the libeler through either negligence or actual malice; and (6) that the defamation caused injury or harm to the plaintiff. The general harm caused by defamation is identified as being ridiculed, shamed, hated, scorned, belittled or held in contempt by others, and lowers her in esteem of a reasonably prudent person due to the communication of the false statement.

According to Jameson (2008), although traditional defamation law may be applied to Internet communication, the current law's application to OGHV behaviors is inadequate for numerous reasons. First, as established in the *New York Times* case, the law only protects a person from the dissemination of false and reputation damaging information: defamation law does not protect individuals from being the target of harassment, which—among previously discussed behaviors—can include negative opinions, criticism, and insults (Jameson, 2010,

p.247). This means that the specific statements used in the case are extremely important, which many OGHV perpetrators use to their advantage. For example, defamation provides an insufficient remedy for cyberbullying victims as defendants can argue that their statements are opinions, and hence not defamatory and protected under the First Amendment (Manuel, 2011, p.232). An online abuser calling his victim a "disease-riddled prostitute" is a verifiable statement (if the woman is not a prostitute nor has diseases), but repeatedly calling someone a "bitch" or "skank", or negatively commenting on the character of the individual—even to the point that it causes extreme emotional distress and negatively affects the individual's offline relationships—is a matter of opinion, and therefore protected speech (Marwick & Miller, 2014, p.7).

Second, application of traditional defamation law to the Internet is difficult because, more often than not, plaintiffs do not know the identity of their abusers. Further, the process of identifying the perpetrator can be time-consuming and often impossible. According to Marwick and Miller (2014), to identify the perpetrator, the plaintiff will need as much information as possible about the poster of these comments. This can include finding the IP addresses which were used to post the messages, and any personal information associated with the account used to post the messages (p.12). However, this information may not be publicly available, forcing the victim to get the information from the ISP, most of whom will not voluntarily disclose a user's confidential information, whether to protect the user or to comply with data privacy laws (Marwick & Miller, 2014, p.12). The victim will thus need a court order forcing the ISP to disclose such information (*Cohen v. Google,* 2009). However, in *McIntyre v. Ohio Elections Commission* (1995), the Supreme Court held that First Amendment protection extends to a writer's decision to speak anonymously, and that the court must carefully consider whether to order the unmasking of an anonymous speaker (Jameson, 2008, p.239; Marwick & Miller, 2014,

p.12).

The court-created tests OGHV victims must undergo to merely find the identity of their abuser to file a defamation claim can be onerous. While various tests exist, most include the same elements (Marwick & Miller, 2014, p.12). Courts may require that the victim take steps to alert the defendant that he may be subject to a court order, such as sending a private message to their account or publicly posting notices where the defamatory content was published. The court may also require that the defendant be given a reasonable amount of time to respond, allowing the defendant time to hire counsel and take steps to formally oppose the motion (Marwick & Miller, 2014, p.12-13). Courts will then consider whether the victim has provided enough evidence to support each of the individual elements of the defamation claim, including how strong the claim would be up against a motion to dismiss. All the while, the defamatory content online can still proliferate and cause harm to the victim.

The likelihood of a plaintiff succeeding in meeting each prong of a libel claim is also slim (Jameson, 2008, p.248). For example, many OGHV victims face obstacles in defamation claims if the communication involved is done privately, such as through email and private messages (Manuel, 2011, p.233). In these cases, the element of publication would not be fulfilled unless done through a blog, website, or public social media platform. According to King (2010), it may also be difficult for cyberbullying victims to prevail under the tort. Although many cyberbullying communications would logically fit the definition of defamatory material because it harms the reputation of another by making false statement to a third person, to succeed on a defamation claim, a plaintiff must prove that the statement (a) was false, and (b) caused material damage to her reputation. Both requirements are high hurdles, especially for young teens whose abuse "often includes opinions, taunts, or sexual innuendo that, while harmful, may be difficult to

refute factually" (King, 2010, p.852-853). Further, proving reputational damage and subsequent injuries is hard for these individuals who have yet to develop professional reputations in the community (King, 2010). Finally, the victim would have to overcome the barrier of presenting evidence that a "reasonable reader" would have believed that the challenged statements conveyed facts about the victim. According to Manuel (2011), in the case of adolescents, they "may believe that insults made against them portray how all of their peers view them, and may take seriously statements that mature, reasonable, adults may not" (p.234). Thus, a discrepancy between the victim's feelings of defamation and the court's perception of the material is persistent throughout the tort's usage.

A key example of this is the case of *Finkel v. Dauber* (2010). Four of Finkel's former classmates created a Facebook group called "90 cents short of a dollar", alluding to the plaintiff, Denise E. Finke's, nickname "11th cent". Finkel sued the former classmates, their parents, and Facebook for defamation. Finkel claimed that the content falsely asserted or implied that she had contracted AIDS**,** had sex with various animals, shared needles with heroin addicts, and had engaged in activities with a male prostitute (Finkel v. Dauber, 2010):

> "BTW the 11th cent, unbeknownst to many, acquired AIDS while on a cruise to Africa (with another member of the group who we shall leave nameless). While in Africa she was seen fucking a horse. NICHTE NICHTE eleventh cent! I mean you know…I kinda felt bad for the eleventh cent...but then again I felt WORSE for the horse…"
>
> "In regards to the 7th cents comment…it was not from an African cruise…it was from sharing needles with different heroin addicts, this led to cross 'mojination' which caused the HIV virus…she then persisted to screw a baboon which caused the epidemic to spread."

> "i heard that the 11th cent got aids when she hired a male prostitute who came dressed as a sexy fireman. apparently…she was lonely, because her friends no longer associated with her. her sexy fireman prostitute was her only company. in addition to acquiring aids, this nameless 11th cent aquired crabs, and syphillis."

However, the Supreme Court of Nassau County sided with the defendants, stating that the postings did not fulfill the claim of defamation. The court reasoned that a "reasonable reader" would not believe any of the statements made in the group about Finkel, and that "while the posts display an utter lack of taste and propriety, they do not constitute statements of fact…taken together, the statements can only be read as puerile attempts by adolescents to outdo each other" (*Finkel v. Dauber,* 2010; Manuel, 2011, p.233). Such a ruling overlooked how adolescents may "believe that insults made against them portray how all of their peers view them, and may take seriously statements that mature, reasonable, adults may not" (Manuel, 2011, p.233-234). Thus, victims of OGHV who attempt to sue for defamation may not only fail to file a suit, but also continue to be belittled and subjected to abuse.

Intentional infliction of emotional distress. For many victims of OGHV, scholars and commentators alike have posited that if the content victims receive is so abusive as to cause emotional torment, turning to the tort of intentional infliction of emotional distress ("IIED") could address their harms. According to Zharkovsky (2010), the tort developed based on the idea that mental injuries (anxiety, grief, rage, etc.) were akin to physical injuries (p.204). There are four necessary requirements for an IIED suit: 1) the defendant must act intentionally or recklessly, 2) the conduct must be extreme and outrageous, 3) and this conduct must be the cause 4) of severe emotional distress. In order to protect the First Amendment, previous court decisions have concluded that only speech on "purely private matters will receive less stringent protection

because the threat of liability would not risk chilling the meaningful exchange of ideas" (Citron, 2014, p.214). As such, Citron (2014) argues, "liability for most cyber harassers' intentional infliction of emotional distress would comport with the First Amendment" as the content is "not engaged in debates about social, cultural, or political issues", but instead "highly intimate, personal matters of private individuals (p.216).

Although IIED could be considered one of the better torts to file against a perpetrator, there are still gaps within the statute that could leave many OGHV victims without redress. First, what can be considered "outrageous" conduct is frustratingly vague. Because case law requires that victims suffer a "severely disabling emotional response" or "unendurable distress"—both of which are also, by definition, vague—courts' decisions in ruling what counts as "outrageous" can be extraordinarily subjective. According to Zharkovsky (2010), actions that would lead an average member of the community to find something outrageous changes between different generations and social attitudes (p.207). Judges, therefore, may perceive the outrageousness of the conduct differently than the claimant, allowing for a perpetrator to avoid the suit. The context in which the supposed "outrageous" communication was conducted can also skew judges' opinions. Such contexts include whether there was an "authoritative relationship between the two parties", whether there "has been a pattern of harassment", and whether the conduct "took place in a public or private sphere" (Zharkovsky, 2010, p.208). For example, OGHV perpetrators can claim that their conduct does not constitute as "outrageous" based on the online environment. As previously discussed, offensive and gendered behavior is a common occurrence online; the perpetrator can claim that their conduct was no more "outrageous" than other users and point to their lack of prosecution to bolster his case. The voluntary nature of the Internet also "makes it difficult for a plaintiff to rebut a defendant's standard defense that a victim assumes the risk of

harassment" and its emotional tolls when she enters the "wild west" environment of the Internet (Jameson, 2008, p.248). Because of this, offenders' vitriolic actions may not be seen as intentional or reckless as "different environments yield different expectations of acceptable behavior" (Zharkovsky, 2010, p.208), and thus bar the victim from winning the suit.

Past cases have also set a precedence where the suffering felt by victims of sexual harassment and discrimination are not deemed severe enough to fulfill IIED's requirements. Most notably, this precedence was set in the offline sexual harassment case *Smith v. Amedisys Inc.* (2002): Lori Smith charged her former supervisors Promod Seth, Mitchell Morel, and William Borne for intentional infliction of emotional distress alongside charges of sexual harassment, discrimination, and retaliation after being forced to resign from the company. Smith claimed that she felt "angry embarrassed, disgusted humiliated and horrified" when Seth made physical and verbal advances towards her—including pulling her down onto a bed during an overnight work trip—and that the sexually oriented statements made by Morel "made her feel as though "she was only hired to work for Amedisys because of her appearance, as opposed to her intelligence and experience" (*Smith v. Amedisys Inc.,* 2002). Smith testified that her treatment led her to become depressed and angry, and caused her painful headaches and loss of appetite after which she consulted a family practitioner and neurologist. However, the court found that Smith's duress was not "unendurable". Despite the acknowledgement that sexual harassment and discrimination has severe mental and physical effects on victims, the court held that "persistent sexual and physical harassment resulting in anger, humiliation, and embarrassment failed to meet this threshold requirement" (Cecil, 2014, p.2530). In summation, Smith's distress in being sexually harassed was not "extreme" enough to warrant the behavior as being "outrageous", regardless of its illegality under Section VII. Based on this precedent, victims of OGHV

behavior may struggle "to prove that their own humiliation qualifies as severe harm under the law" (Cecil, 2014, p.2530).

Due to these gaps in the legislature, combined with barriers posed by money and fear of public exposure, civil torts fail to address the severe forms of OGHV that border on the criminal. In fact, according to Citron in an interview with the *Atlantic* in 2014, she "can only think of three or four reported cases in America, where victims have successfully been awarded a monetary judgment against their online harassers" in civil suits (para.10).

Criminal Law

As opposed to civil torts, criminal charges are formal accusations made by a governmental authority asserting that somebody has committed a crime. Individual states and the federal government each have their own criminal codes defining types of conduct that constitute crimes. While most individuals who are charged under state laws are prosecuted within that state, federal crimes—outlined in Title 18 of the U.S. Code—deal with activities that either extend beyond state boundaries or directly impact federal interests. However, despite the range of criminal charges theoretically available to OGHV victims, barriers to justice are posed by restrictions on law enforcement and prosecution schemes and gaps in criminal law requirements.

Inadequacies in law enforcement and criminal prosecution schemes. When OGHV behaviors reach the severity of criminal behavior, victims often turn to criminal law to address their abuse. When victims are harassed, stalked and fear for their lives, it is the expectation of many that their distress will be addressed by law enforcement, and that suitable charges will be brought against their abusers. This expectation however, is not always met. Problems with jurisdiction and inadequate technological knowledge among officers are serious barriers for victims in need of criminal prosecutions.

Jurisdiction. One of the biggest hurdles in OGHV investigations and prosecutions is jurisdiction (Ahlgrim, 2015, p.10). Although almost every state has laws that criminalize some form of online sexual harassment and/or cyberstalking, they differ in approach and statutory requirement (Cox, 2014, p.4; Marwick, 2014, p.24). Some states' laws explicitly punish perpetrators for harassment over electronic mediums while others amend existing anti-harassment statutes, and still others have criminalized multiple forms in one overly inclusive law (Cox, 2014, p.4; Jameson, 2008, p.256; Schwartz, 2009, p.418). Further, some states have not criminalized online sexual harassment and cyberstalking in *any* statutory form (Cox, 2014, p.4; Jameson 2008, p.256; Shimizu, 2013, p.120), creating unequal protection for citizens who live in different states. For example, while all states have stalking laws, only a few have updated those laws to include cyberstalking. In states with specific cyberstalking laws like California, Illinois, and Massachusetts, theoretically victims can press criminal charges against their online stalkers. However, for those living in a state without these laws, there is little recourse (Sweeny, 2014, para.12).

Differences in statutory definitions and procedures further hampers prosecution of OGHV when the victim and perpetrator reside in different states (Ahlgrim, 2015, p.10; Roberts, 2008, p.281). Many questions arise when abuse crosses state and international lines: what happens if the offender sent threatening and harassing messages from several different states? Which agency has jurisdiction in the case? Is there a case given the decided jurisdiction's definition of the crime? Before any action can be taken, it is imperative that these issues be answered. According to Brenner and Koops (2004), cybercrimes that happen in different states and countries have the potential for both negative and positive jurisdiction conflicts. Negative jurisdiction conflicts occur when no state or country claims jurisdiction over a cybercrime, while

positive jurisdiction conflicts occur when more than one agency claims jurisdiction (p.40-41). For victims, negative jurisdiction conflicts are the worst outcomes to their claims, as their abuse is essentially ignored and the perpetrator goes unpunished. Positive jurisdiction conflicts also create challenges for investigators, especially if the decision ultimately leads to the investigation being conducted in two separate locations. Conducting investigations different jurisdictions is naturally more time-consuming and complicated than it is in only one jurisdiction (Ajmani, 2011, p.316). The amount of time it takes to decide these jurisdictional issues also allows for the offender to continue their actions or erase the evidence before it can be seized (Fusco, 2014, p.26).

Although there is no single rule for where the case is to be brought after the investigation, states generally favor bringing an action in the state where the defendant was located when he sent the messages (Cox, 2014, p.8). For example, there are several state cyberstalking laws that require the offender be present in that state in order to be convicted. These laws "prevent a state from bringing charges in their state when the defendant lives out of state" (Cox, 2014, p.9) and acts as guard for the offenders. For example, an offender in Ohio cannot be charged under Texas law with cyberstalking if their victim resides in Texas because the offender himself is not located in Texas (Fusco, 2014, p.27). Depending on the state the perpetrator resides this, this could lead to no criminal charges being filed in either state. To complicate the matter, some jurisdictions may also deny or ignore extradition requests (Roberts, 2008, p.281). In states that would prosecute the offender however, victims would still be required to spend more of their money on traveling to the state to testify

Inadequate technological knowledge and training. With specific regard to law enforcement, arrest of an OGHV perpetrator may prove difficult in the face of officers'

technological disadvantage or ineptitude. As mentioned previously, many police departments have yet to create a cyber crime division, while many law enforcement personnel face limited resources and lack technical expertise in how to handle the new medium (Marwick & Miller, 2014, p.7; Wexler, 2014, p.10). A key example is the case of Amanda Hess, a female journalist who received the following threatening message via Twitter while vacationing in Palm Springs: "Happy to say we live in the same state. Im looking you up, and when I find you, im going to rape you and remove your head…You are going to die and I am the one who is going to kill you. I promise you this" (Hess, 2014, para.2). Looking at the Twitter feed, it appeared that the account had been made for the sole purpose of sending death threats towards her. Hess called the police who, after interviewing Hess about the incident, responded "What is Twitter?". The officer also dismissed the cyberstalker's statements that he lived in her state and had plans to seek her out at her home as just another online ruse, stating; "This guy could be sitting in a basement in Nebraska for all we know." (Hess, 2014, para.4, 22). In fact, according to Hess (2014), the first time she reported an online rape threat to police in 2009, the officer dispatched to her home asked "Why would anyone bother to do something like that?" and declined to file a report (para.22).

The inability for police officials to understand not only new social media communication methods but the Internet itself is not uncommon. Too many police officers react to reports of online harassment and violence in one of three ways: "by saying 'just turn off the computer'; claiming ignorance of the technology used to threaten a victim; or simply being unaware that there actually are laws against 'true threats" online'" (Dahl, 2014, para.8). Further; "Anecdotal evidence is that the overwhelming number of victims who report online threats are met with indifference or a lack of understanding about how these technologies work" (Dahl, 2014,

para.10). In an interview with the online magazine *Jezebel*, Citron stated that the problem starts with a lack of technical skills and training for law enforcement officers at the local level; "The police response comes from a place of intimidation. The technology just intimidates people, and when police officers are intimidated, they say, 'Turn it off and ignore it'. You have officers who mean well, but they do not understand the technology and they aren't well-trained in the laws" (Merlan, 2015, para.92). In many locales, police work is also still a largely analog affair; 911 calls are immediately routed to the local police force where the closest officer is dispatched to respond, many of whom still take notes with pen and paper (Hess, 2014, para.20).

Even in cases where officers may have a better grasp of online communication, finding and arresting offenders can prove difficult. OGHV offenders, especially cyberstalkers, frequently have greater technical ability than victims and law enforcement agents. For smaller stations, computers may be out-of-date, and officers may not be trained in how to run programs to find IP addresses and crack anonymity programs. Police may also have difficulty in working with Internet service providers ("ISPs") to obtain information on OGHV offenders as ISPs are not required to release personal information to the police. When police agencies have few other ways to identify the online perpetrator, offenders are free to remain anonymous and continue their abusive behavior (Ahlgrim, 2015, p.9; Roberts, 2008, p.280).

Criminal law requirement gaps: "credible threat" and "intent". Criminal charges can be difficult for police to enforce due to the legislative gaps written into federal and state law. According to Citron and Franks (2014), the first hurdle is that criminal harassment and stalking laws only apply to defendants who engage in repeated harassing acts (p.362). Thus, under this study's definitions, cyberbullying and online sexual harassment are prosecuted under criminal law only if it is a part of a cyberstalking campaign.

Additionally, criminal laws contain gaps and loopholes that allow for offenders to escape prosecution. According to Levendowski (2014), harassment laws typically require the aggressor to communicate (or cause communication) directly with the victim in a way that is likely to cause annoyance or alarm (p.432). However, this ignores severe forms of harassment where communications, especially of a sexual nature, includes threats. To be found guilty of stalking on the other hand, an aggressor must intentionally engage in a "course of conduct" that is likely to cause fear of some material harm, with most states interpreting "course of conduct" to mean that the behavior is repetitive or ongoing (Levendowski, 2014, p.432). If the cyberstalkers actions do not comport with a statutes specific definition however, criminal charges will not be filed.

Within most cyberstalking and harassment laws, arresting and prosecuting a perpetrator involves two key requirements: "credible threat" and "intent". According to Markey (2013), conviction of cyberstalking requires a credible threat of harm, while intent to cause harm plays more of a key role in convictions of cyber harassment (p.34). Although credible threat and intent may seem reasonable, applying these requirements to cyberspace and OGHV behaviors is not only difficult, but at times impossible.

Credible threat. In prosecuting criminal cases of OGHV, police have difficulty in establishing credible threat. According to The United States Court of Appeals for the Sixth Circuit, "credible threat" is defined as "any communication that would cause a reasonable person to fear for their physical safety" and "would perceive such expression as being communicated to effect some change or achieve some goal through intimidation" (Cox, 2014, p.6). Though the definition of credible intent—and by extension threatening behavior—may seem clear, there are various gaps within it that allow for OGHV perpetrators to avoid prosecution.

First, credible threat requires that the defendant send an "*explicit"* threat to the victim.

This criterion creates a legal loophole for offenders in that they can—and often do—engage in conduct that does not explicitly threaten victims but would still cause a reasonable person to fear for their safety (Ahlgrim, 2015, p.9; Ajmani, 2011, p.320; Goodno, 2007, p.136; Levendowski, 2014, p.432). Abusers who send vitriolic messages, post doctored photos or revenge porn, and make an effort to follow and harass the victim when online are excused from the "credible threat" requirement if police cannot find evidence of an "explicit" threat. An individual who, for example, posts nude photos of their ex along with her contact information can slip between the true threat requirement even if the victim fears they are at risk of offline attack. Because the post does not explicitly tell viewers to stalk or harass the woman, the post would not be deemed "credible" because threat of a physical attack is not "explicit". Regardless of how damaging the material may be to a victim's professional, economic, emotional and personal life, or how frightened the victim may become, without the "explicit" threat abusers are free to continue their activity.

A major factor of this is the issue of "receipt", or how the message was viewed by the victim. Many laws credible threat requirement states that the communication must be *directly* from the stalker to the victim. However, with the use of private emails, pictures, message boards and Internet forums, OGHV perpetrators can easily post terrifying messages without ever being in direct contact with the victim (Ajmani, 2011, p.321; Goodno, 2007, p.138). Courts may find it hard to perceive such communications as attempts to "effect some change or achieve some goal through intimidation" if the message was not sent directly to the victim. When posted on public forums, courts may interpret these types of messages individuals expressing their feelings or desires rather than threatening communications.

One of the most cited examples of this policy gap is *United States v. Alkhabaz (1997)*.

Jake Baker (also known as Abraham Jacob Alkhabaz), an undergraduate student attending the University of Michigan in Ann Arbor, was a regular contributor of sadistic fictional "short stories" intended for public dissemination and comment via a Usenet electronic bulletin board. Baker's stories attracted the attention of an individual who called himself "Arthur Gonda," a Usenet service subscriber residing in Ontario, Canada, who shared similar proclivities. Baker and Gonda exchanged at least 41 emails detailing a plan for the two men to meet and engage in a real-life depiction of their fantasies to rape, torture, and murder. On January 9, 1995, Baker publicly disseminated online a story in which a woman in his class was tortured, raped, and murdered by himself and Gonda:

> "I yank her up by the hair and force her hands behind her back. I quickly get them restrained with duck [sic] tape. Her little body struggles against me as she screams for help. Jerry tears off her panties and shoves them into her delicious mouth, securing them with a tight strip of rope… Then, Jerry and I tie her by her long brown hair to the ceiling fan, so that she's dangling in mid-air…Jerry tells me her curling-iron's ready. Jerry unplugs it and bring [sic] it over. After taking her down and tying her hunched over a chair, Jerry strokes the device against her bleeding ass cheeks. The heat from it gives her ass small burns…Leaving the iron up her asshole, Jerry reached out, pulled one of her small tits away form [sic] her body. Jerry took his knife, and cut her nipple off. She gags on my cock some more, and I pull out just in time to cum all over her pretty face…So we got the gasoline and spread it all over [full name omitted]'s apartment. We chucked it over her. It must have burned like hell when it came into contact with her open cuts, but I couldn't tell. Her face was already a mask of pain, and her body quivered fiiercely [sic]. "Goodbye, [first name omitted]' I said, and lit a

match…" (United States v. Alkhabaz, 1997).

After Baker's story was brought to the attention of University of Michigan authorities, he was arrested and determined to be a threat to the female student, as well as the rest of the student population. A search of Baker's computer revealed the emails between Baker and Gonda. While Baker was not prosecuted for his online story, the emails between himself and Gonda led to his arrest by the FBI and charges of violating 18 U.S.C. § 875(c), the Interstate Communications Act with six counts of communicating via interstate or foreign commerce threats to kidnap or injure another person.

Despite the graphic detail of the emails between Baker and Gonda, The Sixth Circuit held that the communications did "not constitute 'communication[s] containing a threat' under Section 875(c), reasoning that "even if a reasonable person would take the communications between Baker and Gonda as serious expressions of an intention to inflict bodily harm, no reasonable person would perceive such communications as being conveyed to effect some change or achieve some goal through intimidation" (United States v. Alkhabaz, 1997). This was due to the emails never being directed towards another individual. In spite of the dissent's argument that a "threat" does not have to be directed at an individual, but rather would lead a reasonable, objective recipient to believe that the writer was serious about the threat (United States v. Alkhabaz, 1997), the majority deemed that Baker and Gonda's emails were "shared fantasies that could not possibly amount to a true threat" (Levendowski, 2014, p.433; Marwick & Miller, 2014, p.11). *Alkhabaz* not only demonstrated the high burden to determine a "true threat," but also set a precedent for most hostile online speech failing to meet the standard of credible threat determined by the Sixth Circuit (Marwick & Miller, 2014, p.11).

A second problem with credible threat is that it requires the victim to prove that the

communication instilled in the addressee a fear of "imminent" and serious personal violence from the speaker, and that the offender had the "present ability" to carry out the threat (Ajmani, 2011, p.322; Goodno, 2007, p.138, Cox, 2014, p.5). There are several problems for police and prosecutors when trying to show "apparent ability". First, the anonymity of the offender is the greatest hurdle to overcome. If the victim does not know who is threatening her, and by extension where he is located, the victim will have little ability to determine how imminent the risk of violence truly is, and whether the perpetrator has the ability to carry out the threat (Ajmani, 2011, p.323-324; Cox, 2014, p.5). Second, language communicated in cyberspace is "inevitably delayed, and the receiver or viewer of the speech does not 'hear' the speech while it is being communicated (Ajmani, 2011, p.323). Ascertaining whether a threat is imminent and if the offender had the present ability to carry out the threat at the moment that he "speaks" is infeasible. The victim not only cannot ascertain through voice whether the threat is serious, but may also not even view the speech until hours, days, or weeks after the offender "spoke" (Ajmani, 2011, p.323). Especially in times when victims may not even have known of the threat, it is unfair to place on them burden of proof to show that at the time the threat was made the offender had the ability to carry it out.

Intent. One of the most difficult parts of convicting OGHV offenders of a criminal charge is proving that they had the "intent to cause harm" or instill fear in the victim (Fusco, 2014, p.29). Currently, there are two types of intent that criminal law recognizes: general and specific intent. After the court's ruling in *People v. Owens* in 1983, general intent was defined as the intent to do that which the law prohibits—it is not necessary for the prosecution to prove that the defendant intended the precise harm or the precise result that occurred (Abril, 2007, p.17). Specific intent on the other hand refers to a *particular* state of mind that *seeks to accomplish* the

precise act that the law prohibits. In other words, the prosecution must show that the defendant purposely or knowingly caused the harm at issue.

Intent can be difficult to prove in cyberstalking and online sexual harassment cases because many statutes require that the perpetrator *specifically intended* to harass or threaten the victim. According to Cox (2014), current laws on cyberstalking and online harassment require the offenders to intend, through their conduct, to place the victims in fear of their safety or for their lives (p.5). However, it can be difficult to show specific intent. Because intent is a state of mind, it can rarely be proven with direct evidence and ordinarily must be subjectively inferred from the facts of the case. Regardless of whether the victim suffers emotional or mental stress caused by the offender, if it cannot be proven that the suffering was intended, then the offender cannot be charged (Fusco, 2014, p.29-30).

A recent case in the United States Supreme Court highlights this problem. In *Elonis v. United States*, the Supreme Court reversed the conviction of a Pennsylvania man who directed brutally violent language against his estranged wife. The man, Anthony Douglas Elonis, was in the process of a divorce and made a number of public Facebook posts that detailed self-styled "rap lyrics" that included what many considered to be threatening language:

> "Did you know that it's illegal for me to say I want to kill my wife? . . .
>
> Um, but what's interesting is that it's very illegal to say I really, really think someone out there should kill my wife. . .
>
> But not illegal to say with a mortar launcher…
>
> I also found out that it's incredibly illegal, extremely illegal to go on Facebook and say something like the best place to fire a mortar launcher at her house would be from the

cornfield behind it because of easy access to a getaway road and you'd have a clear line of sight through the sun room. . . ." (Elonis v. United States, 2015, p.3)

After viewing the posts Elonis' soon-to-be ex-wife felt extremely afraid for her life, and obtained a restraining order against him. Elonis' reply to the order was just as violent:

"Fold up your [protection-from-abuse order] and put it in your pocket

Is it thick enough to stop a bullet?

Try to enforce an Order

that was improperly granted in the first place

Me thinks the Judge needs an education

on true threat jurisprudence

And prison time'll add zeros to my settlement . . . (Elonis V. United States, 2015, p.4)

Elonis further wrote that he would like to see a Halloween costume that included his wife's "head on a stick", wanting to make a name for himself by carrying out a school shooting, and fantasizing about killing an F.B.I. agent when he wrote he wanted to; "Pull my knife, flick my wrist, and slit her throat" (Liptak, 2015, para.8). Elonis was eventually arrested and charged with five counts of violating 18 U.S.C. §875(c). Elonis maintained that his posts were merely "rap lyrics" expressing his frustration and anger, and that he had no intent to carry out any of the described activity.

While the district court and circuit court of appeals convicted Elonis on four of the five counts, the Supreme Court reversed Elonis' conviction in an 8-1 decision. Chief Justice John Roberts Jr., writing for the majority, said "prosecutors must do more than prove that reasonable

people would view statements as threats. The defendant's state of mind matters…" (Liptak, 2015, para.2). Chief Justice Roberts further declined to address whether a mental state of recklessness would also suffice. Thus, even though Elonis' wife feared for the lives of herself and her children, without proof that Elonis *specifically intended* to kill or otherwise harm these individuals, he could not be charged with a crime. The new precedent also left victims, attorneys and courts uncertain where the legal line is drawn for a defendant's state of mind.

Internet Service Providers and Section 230 Immunity

Many OGHV victims' primary goal is to have the abusive communication removed from cyberspace as quickly as possible. Victims commonly turn to Internet Service Providers ("ISPs") and website administrators for help, as they are important sources of deterrence and remedy. Their authority gives them the power to allow users to connect to the Internet, moderate discussions, adopt clear behavioral guidelines, and suspend or "banish" users who do not comply with a sites norms and conditions. According to Citron (2014), because ISPs and website operators control what is appearing on their sites, they could minimize the harm by removing or de-indexing abuse before it spreads across the Internet (p.168).

However, gaining the cooperation of ISPs and website administrators can be difficult due to their immunity under Section 230 of the Communications Decency Act of 1996 ("CDA"). Fearing that holding service providers liable for comments left by third party users would lead to ISP overreach and infringe upon free speech, the act states that "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" (47 U.S.C. §230) as long as the service did not provide substantive or editorial contributions. "Interactive computer service" is defined broadly in the statute to "include websites, message boards, instant messenger services, blog

hosting services, and other internet based services including Facebook, MySpace, YouTube, Google, Yahoo, Tumblr, Flickr, Twitter, and even revenge porn" (Marwick & Miller, 2014, p.14). Overall, Section 230 immunizes these services from lawsuits for defamation, IIED, negligence, gross negligence, unfair competition, and false advertising (Marwick & Miller, 2014, p.14). Congress enacted Section 230 to provide immunity from civil liability for "good faith" efforts by these companies to monitor and restrict illicit content by their users (Jameson, 2008, p.249; King, 2010, p.953). This includes "any action voluntarily taken in good faith to restrict access to or availability of material that the provider…considers obscene, lewd…harassing, or otherwise objectionable" (Zharkovsky, 2010, p.199). This has allowed ISPs to self-regulate without concern of being liable for content that is either overlooked or allowed to remain on the site. ISPs under this provision are even allowed to engage in some amount of reviewing, editing, withdrawing, postponing or altering of content without sacrificing immunity (Levendowski, 2014, p.426; Tungate, 2014, p.174).

Although Section 230 broadly protects websites, it does not give ISPs immunity to host any and all content without concern. Section 230 has no affect on federal criminal law or intellectual property law (47 U.S.C. §230), which allows victims to theoretically find relief in copyright suits. Clause (b) of Section 230 also explicitly states that it is the policy of the U.S. to "ensure vigorous enforcement of federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer" (47 U.S.C. §230). Therefore, although Section 230 "preempts state criminal law, Section 230(e)(1) allows the government to allege federal criminal violations against ISPs" (Tungate, 2014, p.176-177). It is also important to note that Section 230 immunity does not apply if the ISP is an "*information* content provider—any "person or entity that is responsible, in whole or in part, for the creation or

development of information provided through the Internet or any other interactive computer service (47 U.S.C. §230). Immunity does not cover original information or content that an ISP or website operator creates or develops.

Despite Congress' intention for Section 230 to promote website best practices and the free speech of users, the law is not serving the public interest as intended. According to Jameson (2008), numerous court decisions upholding ISP immunity under Section 230 have demonstrated that the statute is overly broad, or at a minimum, has been interpreted unnecessarily broadly by the courts (p.250). Individuals subjected to online harassment and stalking appear to have no claim under the statute as service providers "do not have a *legal* responsibility to moderate or take down content that is harassing or offensive, even if such content violates the site's terms of service" (Marwick & Miller, 2014, p.15). According to Zharkovsky (2010), nearly every time a suit is filed for false or malicious content posted online, ranging from instances of cyberbullying to threats of rape and death, the ISP escapes liability while the creator of the content can either not be found or escapes serious civil and criminal charges (p.210). Meanwhile, the abusive content continues to harm the victim.

Legislative gaps and loopholes in Section 230 have led to the protection of the worst online actors, many of whom allow and at times promote the most abusive behaviors from their users. The following subsections will highlight these issues mainly through the framework of revenge pornography. Such framing is due to revenge porn being one of the most severe online harms inflicted on individuals and ISPs common use of Section 230 immunity in such cases. Gaps in Section 230 consists of barriers posed by copyright law under the Digital Millennium Copyright Act, free speech concerns, and the shielding of malicious websites and web practices from tort liability.

Copyright and the DMCA. Section 230 defenders argue that copyright law under the 1998 Digital Millennium Copyright Act ("DMCA") provides adequate redress for revenge pornography victims. The DMCA was meant to protect copyright holders from rampant copyright infringement occurring online (Tungate, 2014, p.178). Importantly, the immunity granted by Section 230 does not affect intellectual property law, and thus ISPs may be held liable for contributory copyright infringement under Section 512 of the DMCA (Digital Millennium Copyright Act, 1998). Contributory copyright infringement occurs when "one party, with the knowledge of another party…induces, causes, or materially contributes to the infringing conduct of another" (Tungate, 2014, p.179). If the ISP had knowledge or reason to know of the infringement, and yet did not act to remove it, then they could be held liable as a contributory infringer. Exemplified in some revenge porn cases, victims who own their images by taking "*selfies*" can demand removal of the sexually explicit material under Section 512 of the DMCA (Cecil, 2014, p.2526, Levendowski, 2014, p.440). ISPs and website providers who know about the infringing material on their site and yet refuse to act would thus lose their "safe harbor", and could be liable for contributory infringement.

Although copyright under the DMCA may seem a viable option for revenge porn victims, there are some major catches that make its current form ineffective. First, although a victim who takes a "selfie" is the rights holder of the image, under the DMCA "the claimant must certify that he or she is authorized to act on behalf of the owner of an exclusive right and must do so under penalty of perjury" (Cecil, 2014, p.2527). Even if a victim who takes the "selfie" has exclusive rights to the photo or video, she must have proof of ownership (i.e. a *registered* copyright) before even contacting the ISP for removal of the images. Obtaining a registered copyright, however, can be a difficult task that subjects victims to humiliation and notice.

Victims must take the private images of themselves to the Library of Congress to *publicly* register them as copyrighted material. Obtaining the copyright also requires victims to pay the registration fee for their copyrights, a cost that some might not be able to afford.

To further complicate the matter, many revenge porn websites have found methods to out-maneuver takedown notices. These methods include hosting the site on foreign web servers outside of US jurisdiction, or hiding the server altogether (Tungate, 2014, p.179). Copyright infringement takedown notices to international ISPs may also prove ineffective as the ISP may simply refuse to comply with United States law (Cecil, 2014, p.2528). Additional barriers are also in place for those victims who move to sue against the hosting website. First, the victim would have to hire a lawyer in order to file a lawsuit, which is costly both in dollars and time. Such expenses can act as a barrier for some victims who have little monetary income, in some cases due to loss of employment from the distribution of the images. In fact, in many cases revenge porn sites will often ignore requests for removal because "they are not worried about being sued since they know that most victims cannot afford to hire a lawyer" (Citron & Franks, 2014, p.360). Second, according to Tungate (2014), the victim runs the risk of the "Streisand Effect", by drawing more attention to the material the victim is seeking to suppress (p.179). Websites may notify their users of the takedown notice, inducing more abuse from users angry at the victim for trying to take down her images.

Additionally, while the DMCA theoretically protects those victims who personally created their images, no copyright protection applies to victims who did not photograph or film themselves. For nearly 20% of revenge porn victims whose images were captured by another, copyright claims are not available (Cecil, 2014, p.2527-2528). In these cases, it is the photographer, usually the distributor of the revenge porn, who owns the images, and therefore

can legally do what he wants with it (Citron & Franks, 2014, p.360).

Free speech concerns. As mentioned previously, commentators frequently raise concerns against implementing legislation or exceptions that they believe would run counter to the First Amendment by chilling speech. The same argument is made by proponents of Section 230, who believe that any changes would chill the very speech and innovation that the statute has allowed to flourish online (Electronic Frontier Foundation, "n.d."). Because ISPs need not fear litigation due to the section's broad protection, they have no need to censor the content that their users post. Commentators claim that this preserves the "free market", and that the statute adequately eliminates from protection communication in which criminal behavior is involved.

The statute's current standing however has actually contributed to the promulgation of unprotected speech due to ISP and web administrators' refusal to acknowledge threatening communications. In part, this is due to online speech being perceived as "less real" than speech enacted offline. In cases of revenge porn for example, website administrators who continue to host the content may fail to realize the harm the online content is causing the victim's offline life, including psychological damage. Revenge porn and its accompanying messages to victims have ranged from sexual solicitations to threats of rape and murder—speech that can be considered obscenity, stalking, harassment, and imminent and likely incitement of violence, none of which are protected by the First Amendment (Citron & Franks, 2014, p.375). However, ISPs still claim the right to host the sexual images, arguing that the messages are "non-threatening satire", or that, unlike "real rape", words and images on a screen cannot hurt someone (Citron, 2014, p.74-75). ISPs and website hosts have thus been able to circumvent Section 230(e)(1) through the claim that such abusive online communication cannot constitute as real threats, even while victims fear for their lives.

ISPs' inability or refusal to recognize the harms of OGHV has also led to the chilling of speech for women. Subjection to numerous threats and indifference from ISPs has created a digital "Spiral of Silence" that excludes women's voices from online communities. According to the "Spiral of Silence" theory, the willingness to express opinions is influenced by external forces, particularly perceptions of mainstream opinions. When people are unsure whether their opinions are consistent with those of the majority, they are usually reluctant to express these opinions (Luarn & Hsieh, 2014, p.884). When female victims' pleas for abusive content to be taken down are ignored, or they themselves are blamed for their own predicament, they may no longer feel that they have a significant voice online, and will thus withdraw from the Internet. For other women who see the abuse and lack of intervention, fear of a similar incident happening to them can also lead them to withdraw, and even begin restricting activities in their personal life out of fear of having the images later appear online. The loss of female voices and opinions online constitutes a loss for society as a whole as digital communities lose valuable perspectives on some of the most contentious issues. By allowing ISPs to ignore victims' requests for the removal of malicious content, Section 230 immunizes online authorities from taking responsibility for facilitating restrictions on women's rights to free speech.

Shielding malicious sites and practices from tort liability. One final problem with Section 230's immunization of ISPs is that it allows for the proliferation of malicious websites and website practices. Most notably, Section 230 has allowed for the increase of malign, but mostly legal, revenge porn websites—websites dedicated to users posting sexually explicit images of their ex-partners for the sole purpose of humiliation and revenge. According to Levendowski (2014), because websites that traffic in revenge porn do not create the content they post—victims or uploaders create the images—the content is, in the language of Section 230,

"information provided by another information content provider" (p.428). Because revenge porn website administrators are not considered taking on the role of the information content provider, Section 230 protection will apply and render nearly any lawsuit against ISPs for stalking, harassment, defamation, or IIED impossible to win (Levendowski, 2014, p.428).

Even in cases where websites purposely encourage users to post illicit content, courts are still unlikely to find them ineligible for Section 230 immunity (Citron, 2014, p.173). Past lawsuits against websites that host revenge porn or content of its ilk have expanded the actions of ISPs and website providers, allowing them to exercise some discretion over posted text and images without losing protection. Thus, even while website administrators may play a large role in the abusive images existing online and the victim's consequential suffering, no civil lawsuit can punish the administrators or force them to take the content down. A prime example of this is the case of *Jones v. Dirty World*. According to the Sixth Circuit Court's documents, Sarah Jones, a high school teacher and Cincinnati Ben–Gals cheerleader, was the "unwelcome subject of several posts anonymously uploaded to www.TheDirty.com operated by… DIRTY WORLD, LLC ("Dirty World")…and of remarks website operator Nik-Lamas Richie posted on the site" (*Jones v. Dirty World*, 2014). The website allowed users to anonymously upload comments, photographs, and videos of subjects like Jones:

> "Nik, this is Sara J, Cincinnati Bengal Cheerleader. She's been spotted around town lately with the infamous Shayne Graham. She also has slept with every other Bengal Football player. This girl is a teacher too! You would think with Graham's paycheck he could attract something a little easier on the eyes Nik!" (Walz & Rogers III, 2014, para.4)
>
> "Nik, here we have Sarah J, captain cheerleader of the playoff bound cinci bengals... Most ppl see Sarah []as a gorgeous cheerleader AND highschool teacher... yes she's also

> a teacher. but what most of you don't know is... Her ex Nate. cheated on her with over 50 girls in 4 yrs... in that time he tested positive for Chlamydia Infection and Gonorrhea...so im sure Sarah also has both. what's worse is he brags about doing sarah in the gym... football field. her class room at the school she teaches at DIXIE Heights" (Walz & Rogers III, 2014, para.5)

Richie would then *personally select* the posts to be published on the site, and add his own editorial comments: "Why are all high school teachers freaks in the sack?—nik"; "I love how the Dirty Army has war mentality. Why go after one ugly cheerleader when you can go after all the brown baggers" (Walz & Rogers III, 2014, para.6). After discovering the "Dirty Army's" posts, Jones sent several e-mails to Richie asking for them to be removed. After Richie refused, Jones filed suit in federal district court on December 14, 2009, alleging defamation, libel *per se*, false light, and intentional infliction of emotional distress under state tort law. Richie and Dirty World claimed that Section 230 of the CDA gave Dirty World, as a provider of interactive computer services, immunity from suit over material authored by third parties and published on the website.

Although the district court denied Dirty World's motion to dismiss in favor of Jones, Richie and Dirty World appealed to the Sixth Circuit where they vacated the district court's decision and entered a judgment in favor of Dirty World. The Sixth Circuit held that the district court erroneously applied an "adoption or ratification test", and instead adopted the material contribution test from *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC.* They considered Richie to be both a content provider (who has no immunity) and host (who would have immunity). The specific content he provided however, were comments which in themselves did not contribute to the defamation Jones was suing for. Additionally, while Jones

claimed that Richie facilitated and encouraged users to post such content, the court stated that they would not use the idea of "encouragement" to define a content provider. Richie and Dirty World could therefore continue their activities as well as refuse to remove the content harmful to Jones.

Immunity under Section 230 has also led to the proliferation of sites with the sole purpose of hosting malicious content, usually for monetary gain. Revenge porn websites exemplify this as many administrators purposely host the illicit material and then charge victims to take it down. For example, WinByState, a private forum that allowed users to view and submit pictures of nude women, advertised a takedown service that charged $250; MyEx.com removed nude photos within forty-eight hours after being paid $400, and even some of the most notorious revenge porn sites such as Is Anybody Up, Is Anybody Down, and U Got Posted charged victims to take their images—sometimes illegally obtained—off the websites. Although these sites should be considered engaging in extortion (Citron & Franks, 2014, p.369), only a few of the most notable site operators have been prosecuted for any crime. Hunter Moore (Is Anybody Up), Craig Brittain (Is Anybody Down), Kevin Bollaert (U Got Posted) and Casey Meyering (WinByState) faced charges of extortion in 2015 (Hess, 2015, para.1), but it was their acquisition of the photos—through either hacking or posing as another individual—that landed them in court rather than the actual practice of running a revenge porn website for monetary gain.

Under Section 230 immunity, even sites not dedicated specifically to revenge porn can participate in malicious practices for their own benefit. A recent example is Reddit's reaction—or lack thereof—to the release of nude celebrity photos in late August of 2014, an incident coined "The Fappening". Around the time that Gamergate was gaining traction, a large cache of private female celebrity selfies stored on Apple's iCloud service were stolen and distributed

across the Internet. One of the most notable sites for the photos distribution was on an extremely popular subreddit called /r/thefappening, which gained 100,000 new subscribers in the first 24 hours of its existence (Massanari, 2015, p.7). Despite the many DMCA infringement notices filed on behalf of those who were impacted by the hack, Reddit administrators seemed reluctant to take down the pictures. Part of the reason for this may have been monetary: in just six days, subscribers purchased enough Reddit gold (a kind of currency that defrays Reddit's server costs) to run the entire site for a month (Greenberg, 2014, para.2). According to Massanari (2015), there seemed to be "a deep reluctance on the part of the administrators to alienate any part of their audience, no matter how problematic, as it will mean less traffic and ultimately less revenue" (p.12). In fact, the subreddit's ban was not ensured until administrators were informed that some of the photos depicted underage girls, a violation of Reddit's policy prohibiting sexualized images of minors (alienth, 2014, para.9). Regardless of the harm they allow to persist, under Section 230, ISPs and website administrators whose purpose may not be to host OGHV material but still refuse to remove it are immune from being punished.

In summary, shielding ISPs through Section 230 immunity leaves victims unable to recover damages and powerless to stop the harm. According to Zharkovsky (2010), because nearly all social-networking sites encourage and thrive on user-generated content, the less likely it is that ISPs and website administrators will take actions that upset a select portion of their population. Without the intervention of ISPs, the more likely it is that the harmful content posted online will spread and become to hard to control, even by its creator (p.219).

Concluding Remarks about Law and Policy

This analysis does not suggest that these laws and policies are *completely* inadequate for addressing OGHV. Defamation, IIED, and copyright suits have in the past brought relief to

OGHV victims. Law enforcement and prosecution teams have also successfully charged and convicted OGHV perpetrators, and some ISPs and website administrators have blocked and reported abusive users to try and stop the proliferation of their behavior. The First Amendment even has a categorical exclusion where speech integral to criminal activity is not protected (Citron, 2014, p.203). However, because of the gaps in policies, the barriers posed to law enforcement, and the immunity granted to the agents who have the most power in helping thwart the abuse, the current legislature contains too many soft spots to conclude that current laws are effective.

IV. Suggestions for Redress through Law and Policy

Due to the ever-changing nature of technology and its uses, no law will ever be all-encompassing and account for every possible behavior. However, this does not mean that current social attitudes and accompanying laws cannot be improved upon for the foreseeable future. Accordingly, this section focuses on proposing legislative actions that can improve current and future laws. This study argues that all forms of OGHV previously mentioned should be considered criminal actions, and so suggestions for prosecuting offenders will focus only on criminal laws. However, many of the criminal policy suggestions could also be applied to civil tort laws to improve the statutes' protections. In order for OGHV in all its forms to be combatted, policies should be aimed at two key areas: redress and prevention

Redress through Legislation

In response to the before mentioned policy gaps, this study proposes that new legislation of all OGHV behavior should reduce the culpable mental state of the perpetrator, broaden the definition of what constitutes as a credible threat, and uniformly extend jurisdictional reach.

With intent requirements, new legislation should lower perpetrators culpable threshold to include "knowingly, recklessly, or with criminal negligence" behavior (Cox, 2014, p.11). Currently, both federal and state harassment and stalking laws require that the defendant *specifically* intended to cause the victim fear and distress[6]. However, due in part to the Online Disinhibition Effect, defendants may communicate threatening messages without fully intending to or understanding how they cause extreme emotional distress. With such a loophole, many cases have concluded with courts determining there was no "intent". Arguably, such a justification does not excuse the individual's actions, nor negate the harm inflicted upon the victim. To avoid these legal loopholes, the culpable mental state of the perpetrator must be lowered to make these defendants eligible for prosecution. According to Cox (2014), "imposing a lower threshold for penalty should deter defendants from engaging in cybercrimes because they will face punishment if their reckless and negligent behavior violates the statute" (p.11). Moreover, such an approach would focus more on protecting the victim's well-being rather than focusing on the defendant's subjective mindset (Cox, 2014, p.11).

[6] Thirty state statutes require that the communication be made with intent, such as intent to harass, alarm, annoy or threaten. These states are Alabama (Ala. Code § 13A-11-8), Alaska (Alaska Stat. § 11.61.120(a)), Arizona (Ariz. Rev. Stat. Ann. § 13-2916(A), § 13-2921(A)), California (Cal. Penal Code § 422(a), § 653.2(a), § 653m(a)-(d), Colorado (Colo. Rev. Stat. § 18-9-111(1), (2)), Connecticut (Conn. Gen. Stat. § 53a-182b(a), § 53a-183(a)), Delaware (Del. Code Ann. tit. 11, § 1311(a)), Hawaii (Haw. Rev. Stat. § 711-1106(1), § 711-1106.5(1)), Illinois (720 Ill. Comp. Stat. 5/26.5-1(a), 5/26.5-3(a)(1) -(3)), Indiana (Ind. Code § 35-45-2-2(a)), Iowa (Iowa Code § 708.7(a)), Kansas (Kan. Stat. Ann. § 21-6206(a)(1)(B)-(D)), Maine (Me. Rev. Stat. tit. 17-A § 506(1)(B)-(D)), Maryland (Md. Code Ann., Crim. Law § 3-805(b)(1)(i)), Minnesota (Minn. Stat. § 609.795 subdiv. 1(3)), Mississippi (Miss. Code Ann. § 97-29-45(1)(a)-(d)), New York (N.Y. Penal Law § 240.30), North Dakota (N.D. Cent. Code § 12.1-17-07(1)), Oklahoma (Okla. Stat. tit. 21, § 1172(A)(2)-(4), Oregon (Or. Rev. Stat. § 166.065(1)), Pennsylvania (18 Pa. Cons. Stat. § 2709(a)), South Carolina (S.C. Code Ann. § 16-3-1700(B), § 16-17-430(A)(2),(5)), South Dakota (S.D. Codified Laws § 49-31-31(1)-(4)), Tennessee (Tenn. Code Ann. § 39-17-308(a)), Texas (Tex. Penal Code Ann. § 33.07(a)-(c)), Utah (Utah Code Ann. § 76-9-201(2)), Vermont (Vt. Stat. Ann. tit. 13, § 1027(a),(b)), Virginia (Va. Code Ann. § 18.2-152.7:1), West Virginia (W. Va. Code § 61-3C-14a(a)), and Wisconsin (Wis. Stat. § 947.0125(2)(a)-(f)).

Barriers posed by credible threat requirements must also be eliminated by broadening the definition of what constitutes as "credible threat" behavior. As mentioned previously, one of the major loopholes in this requirement is that the threat must be "explicit" and occur through direct communication. However, communication through blogs, personal websites, and other social media avenues have allowed for perpetrators to make their targets feel threatened without the need for direct communication, and without "explicitly" stating they want to cause the victim harm. New OGHV legislation would eliminate this by criminalizing conduct through electronic communications that places an individual in reasonable apprehension or fear of immediate or future harm. "Harm", in this broadened definition, would include the unlawful loss of employment, economic injuries, emotional distress, deterioration of victim's physical and mental health, physical harm or harassment by third-party individuals, and online or offline stalking. Again, this would focus more on the victim's suffering rather than trying to evaluate whether the threat was "explicit". This also takes into account the many technological forms of communication that may make the victim feel threatened even if not contacted directly by the defendant.

Finally, states' jurisdictional reach over OGHV crimes must be extended to ensure equal protection and punishment for victims and perpetrators respectively. As many states jurisdictional statutes focus solely on where the act is committed, prosecutors are prevented from filing charges in the state where the harm was felt (i.e. the victim's state). Combined with unequal OGHV criminalization statutes among states, many perpetrators escape prosecution simply based on their location. New OGHV legislation should allow for the crime to be prosecuted "in the state where the act occurred in whole or in part, where the communications were sent to, where the communications were received, or where an element of the offense

occurred" (Cox, 2014, p.12). In other words, "whether an offender was physically in New York State when a…communication was sent, or whether the victim was physically in New York State when a…communication was received, the crime can be punishable under New York State law" (Fusco, 2014, p.39). With this change, even if the perpetrator were to live in a state with weak OGHV laws, those states that adopt the proposed statute would be able to bring charges against the perpetrator in their jurisdiction. This also eliminates the possibility of negative jurisdiction conflicts (at least within the U.S.) by assuring that the perpetrator can be prosecuted in at least one state.

Further, cooperation between state police departments must be better ensured. Such assurance could come through legislation by adopting an expanded interpretation of the Full Faith and Credit clause of the Constitution. Whether due to authorities lack of understanding of the laws or outright dismissal of the crimes, cooperation among police jurisdictions in OGHV cases has not been held to the same standard as other interstate crimes. The most egregious lack of cooperation is the refusal of some jurisdictions to extradite OGHV offenders upon other jurisdictions' requests. However, the Full Faith and Credit clause provides that "full faith and credit shall be given in each state to the public acts, records, and judicial proceedings of every other state…" (U.S. Const. art. IV, *§*1). The various states must recognize legislative acts, public records, and judicial decisions of the other U.S. states to ensure that decisions rendered by the courts in one state are recognized and honored in every other state. By interpreting "judicial proceedings" to include investigations and charges of OGHV—combined with broadened jurisdictional reach—refusals to extradite the charged individual should amount to not recognizing the legislative acts and judicial decisions of another state, i.e. violating the Full Faith and Credit Clause. Although it would be ideal for different police jurisdictions and departments

to cooperate willingly, ensuring that no perpetrator escapes justice is best ensured through mandatory cooperation statutes.

Cyberbullying criminal law. While currently there are anti-bullying statutes in place to address instances of cyberbullying, policies are not uniform and rarely do those punishments include criminal charges. According to the Cyberbullying Research Center's 2016 review of state cyberbullying laws and policies, legal handling of cyberbullying is not consistent (Hinduja & Patchin, 2016, p.1). For example, some states bullying policies make no mention of "cyberbullying"[7], and differ in how—and even if—to punish offenders who created the material off-campus. Further, many states policies regarding punishment only outline penalties that schools may enforce, such as suspension of expulsion. For many, there is no mention of how police may handle the worst cyberbullying incidents.

Because cyberbullying is not just innocuous teasing, this study proposes that cyberbullying activities which—if performed by adults—would constitute as criminal behavior must be addressed with criminal punishments. Manuel (2011) proposed that the elements of a criminal cyberbullying statute should be similar to that of harassment and stalking, with further italicized elements added to the language of his proposal: the individual (1) *knowingly, recklessly, or with criminal negligence engaged in* (2) malicious conduct, (3) directed at a specific person, (4) which would result in a reasonable person of a similar disposition *to feel alarmed, harassed, intimidated*, *terrified, or threatened,* or face substantial emotional, psychological, or physical harm, including but not limited to psychiatric admission or suicide*,* (5)

[7] Alabama, Alaska, Arizona, Colorado, Delaware, Idaho, Indiana, Iowa, Maryland, Mississippi, Montana, New Jersey, North Dakota, Ohio, Oklahoma, Pennsylvania, South Carolina, South Dakota, Texas, Vermont, West Virginia, Wisconsin, and Wyoming make no mention of "cyberbullying". Georgia, Kentucky and Nebraska have proposed to include it.

through the arena of virtual space, including but not limited to blogs, social networking websites, electronic mail, telecommunication devices, and Internet communications (Manuel, 2011, p.248)[8]. Key here is the requirement that the standard of evaluating the harm is through the perception of an individual *of the same or similar age* if in the same situation. This would account for the discrepancy between the victim's feelings of harm and the court's perception of the material due to age difference. It also takes into account how third parties of the same age, i.e. the victim's peers and community, would view and react to the material. By evaluating whether those individuals would (1) believe the material, (2) be affected by the material to change their behavior towards the victims, or (3) be solicited by the material to engage in the harassment and violence, the specific harms suffered by adolescents will not be overlooked as a trivial matter.

In regards to punishment, those who participate in such behavior should be charged with a misdemeanor and should be "disciplined through community service, counseling, mandatory Internet instructional classes, and/or imprisonment for no more than two years" (Manuel, 2011, p.248). It is important to note that any laws concerning minors will usually be evaluated on a case-by-case basis. While any dealing with adolescents' engagement with OGHV is best done through education, how criminal behavior is dealt with should be based on the language of the communication, the specific effect on the victim, and the severity of the threat posed to the adolescent and overall community. Instances of cyberbullying that involve shaming and exclusion for example, are best addressed through education while instances of sexual harassment, threats, or incitements of violence should be dealt with more severely by law

[8] The study's complete suggestions for criminal cyberbullying legislation can be found under the "Model Law" section.

enforcement. Depending on the nature of the communication, it should be up to authorities' consideration of age, understanding of the incident, and harm done to the victim and community on whether to charge the defendant with a crime.

Online sexual harassment law. The solution to combating the worst forms of online sexual harassment lies in crafting laws that better define and punish the different behaviors. New legislation should clearly define the different forms of online sexual harassment rather than combining all behaviors under one overly-broad law. This not only helps officers discern which behaviors are criminal, but also allows offenders to be charged at different severities depending on their actions. Under Jameson's (2008) proposal, any such legislation should aim to meet three criteria: first, criminalized forms of online sexual harassment should be recognized as harassment towards a person that induces emotional distress; deterioration of victim's physical and mental health; physical harm; and includes the loss of employment; economic injuries, harassment by third-party individuals; and online or offline stalking which occurs over an electronic medium. Second, information that is considered private by reasonable individuals should remain private. Third, the right to free speech should be upheld in situations where the defendant's actions are lawful (p.265). Under these three criteria, any communications that induce the described distress would constitute as "credible threat" behavior, and those who share private images—under any of the new actionable culpable mindsets—would be seen as having "intent" to cause harm. Further, the third requirement upholds citizens' right to post sexually explicit—and arguably offensive and distasteful content—as long as it is protected as free speech. This study further proposes a fourth criteria, where the different forms of online sexual harassment should be punished according to their severity of harm upon the victim, ranging from

a misdemeanor to a felony. Under these criteria, all previously discussed forms of online sexual harassment would be characterized as criminal activity[9].

Revenge porn law. Due to this study's classification of revenge porn as the worst form of online sexual harassment, as well as a sex crime, specific attention must be paid to its legislation. While many states have currently implemented or have begun the process of implementing statutes criminalizing the behavior, certain key components should be taken into account for future legislation. Following the previous suggestions for other forms of online sexual harassment, revenge porn laws should clarify the privacy of the material, "require that the state provide proof of harm against the victim, do away with requiring proof of malicious intent, and create adequate penalties that reflect the severity of the crime" (Citron & Franks, 2014, p.387-389).

Due to the revealing nature of the images, revenge porn legislation should determine whether or not the defendant betrayed the expected privacy of the person in the image, i.e. whether or not the image was expected to be private and the defendant knowingly, recklessly, or with criminal negligence (i.e. with intent) released it to public. According to Citron and Franks (2014), a law could require proof that the "defendant knew that the other person did not consent to the disclosure *and* that the other person shared the image (or permitted the image to be taken) on the understanding it would be kept private" (p.387). To improve on Citron and Franks' suggestion, this study proposes that legislation should classify all sexually explicit or nude images as "private" material *unless specifically stated otherwise*. In other words, without the consent of the depicted individual, any distribution would make the perpetrator liable to both

[9] The specific criminal charges for individual online sexual harassment behaviors is expanded up in the "Model Law" section

criminal and civil prosecution—the civil violation being invasion of privacy. This proposal will allow the courts to determine whether the distribution was an invasion of an expected privacy, something no courts have yet addressed (Levendowski, 2014, p.436). Such a proposal also addresses the issue of the distribution of images when not owned by the victim. With this legislation, even if the perpetrator were the one to take the photos of the victim, without the consent of the depicted individual to distribute the images, the perpetrator would still be liable for civil and criminal charges.

Further, rather than proving that distributors had malicious motive in releasing the images, legislation should focus on providing evidence that the victim consequently came to some form of harm. Proving motive is much too high a barrier for many police and prosecutors to cross, and misunderstands the harm resulting from the action— regardless of the motive of the perpetrator (whether through a desire to be entertained, humiliate, or generate a profit), the distribution of sexually explicit images is a violation of an individual's privacy. As long as the individual knowingly breached that privacy by distributing the explicit content and caused harm to the victim, the motive is irrelevant. According to Citron and Franks (2014), requiring a state to prove that the victim suffered harm could allow the statute to have a better chance of withstanding overbreadth challenges. Victims' "suffering" could be defined as the harms mentioned within this study, such as loss of employment, economic injuries, deterioration of a victim's emotional, physical and mental health, physical or emotional harm by third-party individuals, and stalking.

Along with staunch definitions of what constitutes illegal revenge porn activity, clear exceptions must also be defined in the legislature to avoid overbreadth that infringes on citizens' rights. Specifically, revenge porn bills must include exemptions that guard against the

criminalization of disclosures concerning matters of the public interest (Citron & Franks, 2014, p.388). Laws should make it clear that it is a crime to distribute someone's sexually explicit or nude image if *and only if* those images do not concern matters of public importance such as images in connection with a criminal prosecution, or used in accredited purposes of scientific research and medical or legal documents.

This study further proposes that all forms of revenge porn be categorized as a felony. Penalties for revenge porn have been lacking in adequate punishment for years. Perpetrators have been released with misdemeanors, and at times not even prosecuted, as courts have deemed revenge porn as innocuous. Not only must revenge porn be recognized for its serious harms, but the penalties for those who spread it must reflect its severity. As stated by Citron and Franks (2014), if the conduct is categorized as a mere misdemeanor, it "risks sending the message that the harm caused to victims is not that severe" and "decreases incentives for law enforcement to dedicate the resources necessary to adequately investigate such conduct" (p.389). Thus, it is imperative that nonconsensual porn bills implement more severe punishments to perpetrators. Laws regarding revenge pornography and website operators is expanded upon later in the study.

Cyberstalking criminal law. Cyberstalking statutes should recognize the distinctive features of the Internet that make the behavior so harmful. Specifically, the statute should apply to anonymous and repetitious communications, false impersonation, and expand the definition of "electronic communications" to explicitly include the incitement of third parties on websites and web postings. In all situations, due to the extremity of the harm inflicted on the victim, cyberstalking should be classified as a felony.

To further ensure that cyberstalkers are adequately prosecuted, state cyberstalking laws should abandon requiring proof of imminence found in credible threat requirements. The delay in

the victim viewing the cyberstalkers' activities or messages does not allow for the victim to adequately evaluate how imminent the risk of violence truly is. The inability to ascertain where the perpetrator is located also makes it hard for victims to prove that the perpetrator had the "present ability" to carry out the threat, or show proof of imminent fear even if the fear is reasonable. Eliminating this in the broadened credible threat requirement would create a more effective cyberstalking law that would be based off the reasonable fear instilled in the victims, and any mental, emotional, and/or physical pain or suffering caused by the offender (Fusco, 2014, p.41). If the courts wish to maintain the requirement however, then they must reinterpret the meaning of "imminence". This study agrees with Ajmani's (2011) suggestion that to meet a new imminence standard, the victim "would have to prove a reasonable fear of imminent personal violence *after* he or she viewed the frightening speech—rather than at the time when the alleged cyberstalker sent the message or made the web posting" (Ajmani, 2011, p.326). Again, this would focus more on the victim's fear of an attack—and the emotional and mental harm stemming from such fear—rather than estimating whether or not the attack was likely to occur.

A section of the new cyberstalking statute should also address the different forms of surveillance and invasive technological methods that a cyberstalker can employ. An example of this would be Fusco's (2014) recommendations for New York State legislation that "the cyberstalking law should be worded as to define unlawful surveillance as the repeated act of recording, monitoring, or observing information, such as activities and behavior, for purposes of gathering personal data regarding an individual or group of individuals" (p.40). This could include technologies such as hidden mobile apps, GPS tracking, webcam hacking, and more advanced techniques like traffic analysis, spyware, key loggers, backdoors, viruses, and Trojans. The statute should be worded to include these methods, as well as approaches that are not

specifically listed but could be perceived as techniques of cyberstalking (Fusco, 2014, p.40). In regards to invasive technological methods, the statute should also be worded to address the use of electronic devices to "hinder, stop or invade the online activity of another", in ways that result in a machine or network resource becoming unavailable to its intended users, or the release of information that references a name, domain address, phone number, or other item of information a reasonable person would consider private. Such broad language would encapsulate cyberstalkers use of doxing, DoS and DDos attacks, as well as other methods that may be employed in the future.

States have already begun to implement laws that follow these lines. According to Ajmani (2011), the state of Washington has one of the most effective cyberstalking statutes in this regard as it includes provisions for anonymity, repetitious communication, and third-party communicators (p.323). The statute also reads that "'electronic communication' includes, but is not limited to, electronic mail, Internet-based communications, pager service, and electronic text messaging" (Wash. Rev. Code Ann. § 9.61.260.), providing for a broader reading of what methods of communication cyberstalkers use. The broader language also allows for prosecutors to charge cyberstalkers who incite third-party stalking. Further, the Washington statute also states that "any offense committed under this section may be deemed to have been committed either at the place from which the communication was made or at the place where the communication was received" (Wash. Rev. Code Ann. § 9.61.260.), allowing for a longer jurisdictional reach (Ajmani, 2011, p.328).

Changes in the credible threat requirement have also begun to appear in state legislation. The state of Illinois, for example, has a distinct cyberstalking statute that addresses the specific characteristics of the Internet *and* does not have a credible threat requirement. The provision

states, in part, that a person commits cyberstalking when he or she "creates and maintains a…webpage which is accessible to one or more third parties in order to place the victim in fear, threaten the victim, or solicit third parties to stalk the victim" (720 ILL. COMP. STAT. 5/12-7.5; Ajmani, 2011, p.329). This provision is significant because it addresses, in detail, the various ways in which cyberstalkers can use websites to carry out their mission of controlling and harming victims without directly communicating a threat to the intended target (Ajmani, 2011, p.329). Other states should follow this example.

Section 230 Amendments. ISPs and website administrators arguably have the most power and authority online. They are important sources of deterrence when conducting best practices, and are key to removing damaging content. To ensure their cooperation in OGHV cases, Congress should amend Section 230 to exclude the "worst actors" from its protection, create a revenge porn exception within the statute, and withhold immunity for non-responsive websites to better ensure the protection of victims.

Excluding worst actors. Congress should amend Section 230's safe harbor provision to exclude the the "worst actors" on the web, namely websites that purposefully engage in or encourage forms of OGHV. These sites are specifically those that "encourage cyberstalking or nonconsensual pornography and make money from its removal or that principally host cyberstalking or nonconsensual pornography" (Citron, 2014, p.177). Extending upon Citron's assessment, this study proposes that the amendment would also relate to websites that encourage threatening behavior, coercion, extortion—whether of a sexual nature or otherwise— and unlawful voyeurism, but only if such behavior were the main purpose of the site. The new amendment could mirror Section 230's current exemption of federal criminal law and intellectual

property (Citron, 2014, p.177) and, with this study's own italicized suggestions, could be worded as such:

> "*Nothing in this section shall be construed to exempt from liability* websites or other content hosts that purposefully encourages cyberstalking, *threats of violence, coercion and extortion, including those of a sexual nature*, *unlawful voyeurism* and nonconsensual pornography, and seeks financial remuneration from its removal or that principally hosts *content of such nature*."

This amendment would exclude many "bad actor" websites that purposefully seek to harm individuals with no other contribution to the public. The new addition would not put at risk websites whose users engage in such behavior unencouraged by the website operator, nor websites whose purpose is not tied to hosting the malicious content. For example, Twitter would not fall victim to such an amendment despite the vast amount of OGHV content that can be found on it, as it neither encourages such behavior nor is its primary goal to host or allow it. Any website that falls outside of the amendment's immunity would be subject to the same legal actions as if they were the original poster. Considering the hundreds of claims that could be brought against them, ISPs and website operators would be reluctant to become the "bad actors" of the Internet and purposefully host OGHV content.

Revenge porn exception. The issue of online revenge porn cannot be adequately addressed with only the previously mentioned amendment. Although many websites devoted to revenge porn would lose their immunity under the modified statue, there are many instances of revenge porn appearing on sites whose primary purpose is *not* to encourage or host such content, but may still fail to remove it upon request or prolong the removal process (i.e. "The Fappening"). Congress should therefore create a nonconsensual pornography exception within

Section 230. Although individual states have their own revenge pornography laws, Section 230 (e) states; "No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section" (47 U.S.C. §230), namely that no state civil torts can be brought against websites who continue to host the tortious content. However, as some states have yet to fully criminalize revenge pornography, especially when "created" by the offender, these civil torts are the only forms of redress victims can utilize. To ensure websites subscribe to best practices and help stem the proliferation of the spiteful content, a nonconsensual pornography amendment to the statute must be created. The amendment could read as follows:

> "Nothing in this section shall be construed to exempt from liability websites or other content hosts that allow for the continued hosting of nonconsensual pornography upon notification of its presence. Websites and content hosts will also be subject to the take-down notices of the content submitted to other hosts."
>
> This section does not apply to:
>
> a. Distributions made in the course of reporting an unlawful activity
> b. Distributions made by a law enforcement official in connection with a criminal prosecution
> c. Distributions made by a person acting in compliance with a subpoena or court order for use in a legal proceeding
> d. Distributions made by a person acting with a bona fide and lawful scientific, educational, governmental, or other similar public purpose
> e. Distributions made in the course of a lawful public proceeding

f. The image is of a voluntary exposure in a public or commercial setting[10]

Website operators and ISPs who do not comply with the amendment would lose their immunity, prompting swift action to remove the content and providing the victim with the relief they are seeking. This also prevents civil and criminal courts from having to deliberate whether ordering the website host to take down the actionable material is in violation of Section 230 as the content would not be protected. Requiring that sites remove the content on their domains after being notified of takedown notices on other sites also helps to stem the proliferation of the material. The amendment also protects the free speech rights of posters who submit the content in matters related to the public interest, while excluding from exemptions those that are only meant to harm and humiliate the target.

Non-responsive websites and hosts. This study also proposes that further amendments to Section 230 be added to prompt non-responsive website operators and hosts to engage in best practices that help redress victims' grievances. As proposed by Cecil (2014), the amendment could limit a site operator's immunity by "requiring action upon notice of tortious activity" (p.2548). Failure to act upon notice would abolish the website's immunity. Such amendments are not unprecedented, as seen in Section 512 of the DMCA. To avoid overcompensation by website operators that could lead to censorship of protected speech, this study agrees with Cecil (2014) that the amendment should *only* require action upon notification (p.2549). The amendment could read as such:

> "Nothing in this section shall be construed to exempt from liability websites or other content hosts that do not act upon takedown notifications of tortious material. Websites

[10] Citron & Franks, 2014, p.373

and content hosts have a period of (X amount of time) to remove or disable the material."

The process of notification should be simple to provide less barriers for victims. Website operators should create an online form that allows complainants to describe and submit to a designated agent their legal claim. The website would then have a set period of time to respond to the complaint before their immunity is lost. This both holds the website accountable for inaction, and helps to hinder the proliferation of the content. As proposed by Cecil (2014), elements of the notification would include:

(1) Identification of the actionable material to allow the computer service to locate the content
(2) Information reasonably sufficient to allow the computer service to contact the complainant, such as telephone number, email, etc.
(3) A claim that the listed materials give rise to legal action, such as defamation, invasion of privacy, and intentional infliction of emotional distress
(4) A statement that the complainant has a good faith belief that the use of the material in the manner complained of gives rise to legal action as described in the claim
(5) The physical or electronic signature of the complainant [11]

In regards to the third requirement, this stipulation ensures that existing laws are adhered to, as well as protects website user's free speech. It is common for many netizens to overreact to a comment made by another individual, claiming that their actions are tortious when the communication is merely distasteful to them. Therefore, this stipulation ensures that offensive but *legal* speech and actions online are not viable for action from a takedown notification.

[11] p.2550

To avoid notifications of unpleasant but legal activities, great care must be taken to ensure that only reasonable claims are submitted. One possibility is to include the Section 230 amendment passage and definitions on the notification application. Better yet, the online application's home page could have the amendment, as well as the possible claims and what they require, for the complainant to read. To access the application, the complainant must click on a "*click wrap*" to show their understanding before they are allowed to proceed to the form. Although this would certainly not exclude all outrageous claims, many complainants acting merely in anger will be deterred upon seeing the requirements necessary to prove their claim. A clause may also be added that imposes liability on any individual who "knowingly materially misrepresents" that material is actionable (Cecil, 2014, p.2550) to deter individuals from abusing the notification procedure.

In agreement with Cecil (2014), this study also proposes that to ensure fairness to both parties, the ISP or website operator must first take steps to contact the original poster to allow the individual to remove the content themselves or notify them of its removal (p.2551). To warrant no legal retaliation from the original poster, the terms and conditions of the hosting website should stipulate that they have the right to remove such content upon notification if it comports with the definition of tortious, or other non-protected speech or activities. Records of when the communication was posted, who it was communicated to or about, and when it was removed should be kept by website providers as evidence of their actions, as well as to maintain accurate records in case of future legal prosecution. Further, a loss of immunity for a website or host should only occur if the claims that the content is viable for legal action are true. If the website does not meet these requirements and fails to take down the content, the complainant can then sue them as they would the original poster

Prevention through Cultural Change

While legally there must be a movement to improve legislative redress for victims, ample attention must also be paid to policies aimed at preventing OGHV and its effects. To do so, there must be an overall cultural shift in how the public and authorities think about and are educated in online gendered harassment and violence. This shift in viewing OGHV as a societal problem must be accomplished by employing educational policies within three key areas: schools, businesses, and law enforcement.

Schools. To address OGHV with the intent of prevention, it is best to start at its earliest source. School curriculums, such as computer or sexual education courses, can cover material devoted to teaching smart and safe Internet use. According to Barak (2005), such an educational intervention "may review standards of netiquette behavior, together with tips on identifying hostile and malicious communications and impingement of privacy and boundaries" (p.86). It is hoped that for some of these adolescents, educational intervention might change perceptions, attitudes, and values, or at the very least make them aware of the issues and contribute to changing their potential problematic behaviors.

School administrations must also be better educated and more willing to assert protection and punishments. According to Shariff and Gouin (2006), schools may perpetuate hierarchies of power and tacitly condone cyberbullying by refusing to address it (p.8). Within their study, Shariff and Gouin (2006) revealed that when plaintiffs approached the schools for support, school administrators and teachers put up a "wall of defense" and, according to some parents surveyed, school administrators allegedly: "a) assumed that the victims (plaintiffs) invited the abuse; b) believed parents exaggerated the problem; and c) assumed that written anti-bullying policies absolved them from doing more to protect victims" (Shariff & Gouin, 2006, p.9).

This lack of intervention may stem from the school's inability to meet the challenges of cyberbullying due to deficient knowledge about technology and the vitriolic nature of the behavior. Current confusion on school administrations' legal responsibilities in addressing cyberstalking also negatively affects intervention. For example, the lingering vagueness on student speech rights "creates disincentives for schools to tackle the issue aggressively, often making it safer and easier for the school to ignore cyberbullying" (King, 2010, p.875). On the other hand, schools could also find themselves liable under Title IX of the United States Education Amendments of 1972. Much like how Title VII of the Civil Rights Act prohibits sexual and racial discrimination in the workplace, Title IX protects individuals from discrimination by stating; "No person in the United States shall, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any education program or activity receiving federal financial assistance". Under this law, schools can become liable for not preventing cyberbullying when the communications involve sexually discriminatory language. Additionally, it may be hard for school administrations to exert responsibility over the actions of students if the communications are not happening while at school or with the use of school-provided technology.

In response, this study suggests that students should be be liable to school intervention and punishment if: (a) the online content was viewed on campus, (b) the online content was created at school or using school resources, (c) the discussion of the content on campus causes harm to the individual(s), and (d) either the perpetrator or the victim attend the institution. The first, second and fourth factors act as a miniaturized version of the proposed jurisdiction statute for criminal laws. If any of the action or effects of the action, in whole or in part, occurs on campus then the perpetrator is subject to the school's jurisdiction. If a school should be hosting

either the victim or the offender, then they must make an effort to protect or punish the individuals respectively, even if the other party attends another institution. The fourth factor also encourages school administrations to cooperate with each other, creating a vast network of support for victims. The third factor ensures school administrations' acknowledgement of the harm occurring on their campus and, due to cyberbullying's gendered nature, will act to discourage and stop it while not violating Title IX and students' free speech rights.

Under these guidelines, the principal or the principal's designee of an elementary school, middle school, or high school, should investigate when a student reports to any principal, teacher or guidance counselor instances of cyberbullying, including threats of harassment, intimidation, and physical harm to a student's person or property. Following the investigation, the principal or the principal's designee should report the findings, along with any disciplinary action taken, to the director of schools and the chair of the local board of education. This creates a system of accountability, as well as provides precedent for how future cyberbullying cases could be addressed.

To provide better education on cyberbullying to school faculty, at the beginning of the year teachers and school counselors should be provided with a copy of the state and school's cyberbullying policy. This would include information on the policy's implementation, cyberbullying prevention strategies, and instructions on how to address it when it happens. In addition, the department of education should further provide recommendations of appropriate, available, and free bullying and harassment prevention resources. The school administration should also make available to students and parents information relative to cyberbullying prevention programs, and promote discussion with respect to prevention policies and strategies.

All such policy implementations would help foster safer school environments, and would provide better protection to victims of cyberbullying.

Businesses. As previously mentioned, victims have difficulty finding and keeping jobs after searches of their name prominently display their abuse. Employers have admitted to relying on social media information and Internet searches in making hiring and firing decisions. This reliance however, can greatly discriminate against women who are at the most risk of becoming OGHV victims. To ensure that victims are not left out of employment pools, a mixture of education and policy changes should be exercised on employers and their businesses.

First, employers should be educated on the behaviors and consequences of OGHV to both better protect their current employees and refrain from turning away potential new hires. Under Title VII, education in racial discrimination and sexual harassment in the workplace has led to better work environments for women and minorities. The same education can be done for discrimination against victims of OGHV. To ensure that such an environment would continue, the most effective training programs would be repeated often in any worker's training.

From a legal perspective, this study agrees with Citron (2014) that the EEOC "should and could interpret Title VII to ban employers from using search engine results as the basis for denying individual's employment opportunities" (p.183). Better known as the U.S. Equal Employment Opportunity Commission, the EEOC is responsible for enforcing federal laws that make it illegal to discriminate against a job applicant or an employee because of the person's race, color, religion, sex, national origin, age, disability or genetic information. In no way would including victims of OGHV in this protection conflict with current EEOC interpretations: currently, the EEOC has interpreted that Title VII bans employers from using arrest records as the sole basis for rejecting job applicants, recognizing that doing so would "offset the potential

for discrimination because racial minorities disproportionately face arrest" (Citron, 2014, p.183). The same should be done for OGHV victims as searches revealing abuse has a disparate impact on women. By banning employers from rejecting job applicants solely on the basis of the abuse they have encountered online, fewer female victims will be denied economic opportunities.

Even with such an interpretation however, victim's of OGHV may still not be able to combat cognitive biases as employers would contend that the postings had little weight in their decisions. To ensure that this is true, this study continues to support Citron's (2014) approach by suggesting that "if employers use third parties to compile information on prospective employees, including data culled online" they should be required to comply with the Fair Credit and Reporting Act ("FCRA") (p.184). The FCRA requires employers to inform individuals that they intend to take adverse action against them due to their credit report. According to Citron (2014), "this gives individuals a chance to explain inaccurate or incomplete information and to contact credit-reporting agencies to dispute the information in the hopes of getting it corrected" (p.184). By extending the act to employers' evaluation of applicants from online searches, the policy would give OGHV victims the chance to explain their abuse and address any detrimental allegations before it costs them employment opportunities.

Law enforcement. Mandatory training for law enforcement about the different forms of OGHV and legal options for redress must also be implemented as far too often officers fail to address complaints "because they lack familiarity with the law and technology" (Citron, 2014, p.144). According to Fusco (2014), while it is imperative that law enforcement officials know the laws in their jurisdiction, it is also "important that they know how to handle devices incorporated in these laws" (p.42). This means that training should include the most up-to-date knowledge about current technology and forms of communication, especially that of social

media where rising incidents of OGHV are of concern. Training would also include how law enforcement could take critical steps to protect victims and preserve evidence. Cox (2014), for example suggests that "officers should hold detailed interviews with the victim…try to establish exactly when the harassment began and how it was undertaken… collect evidence from the victim's computer and provide a forensic analysis of the data (p.13). Officers should also be trained to know that "in order to preserve as much digital evidence as possible…to not unplug or shut down a running computer, and not to close out any open tabs or applications. The same goes for a cell phone, smart phone, or tablet" (Fusco, 2014, p.42).

Additionally, states should "require police departments to report the number of cyber stalking and online harassment complaints they receive and the outcome of those cases" (Citron, 2014, p.145). Accurate records allow officers to keep track of offenders so as to apply appropriate punishments for multiple offenses. Such records, when shared among different police departments, also allow officials to cooperate better when trying to solve OGHV cases. Publicly releasing the statistics would also allow for societal discussion about "the efficacy of training efforts" (Citron, 2014, p.145), as well as provide more accurate and up-to-date statistics for researchers. Having official statistics could also help dispel the myth that forms of OGHV are "harmless" Internet experiences, which may help deter future perpetrators. For this to happen, states and relevant agencies of the federal government should allocate funding to training and mandatory reporting. Even if no legal suggestions are to be taken to change the current system, through training and improved record keeping law enforcement officials will be better able to enforce existing laws which, although filled with loopholes, might lead to redress for the victim.

Model Law

The proposed model for a comprehensive OGHV statute incorporates the factors previously discussed, and is specific only to the types of cyberbullying, online sexual harassment, and cyberstalking behaviors mentioned within this study. By adopting this improved statute, the likelihood of successful prosecution of OGHV crimes is increased and affords greater protection to victims. The following model law is a compilation of proposed and enacted legislation, as well as this study's own suggestions. These sources of law include: 18 U.S.C. § 1030(a)(5)(A), 18 U.S.C. § 1030(a)(7)(A), Arizona penal code § 5-71-217, Cox (2014), Citron and Franks (2014), California Penal Code, Title 15, § 647, Fusco (2014), and Louisiana Penal Code Title 14, RS 14:40.7.

TITLE #, Section #- *Online Gendered Harassment and Violence*

I. Cyberstalking. A person commits cyberstalking by intentionally, knowingly, recklessly, or with criminal negligence doing any of the following:
    a. Without lawful authority, on at least two separate occasions sends or engages in repeated conduct or communications by means of an electronic communications device which would result in a reasonable person becoming terrified, intimidated, threatened, harassed, suffer serious emotional distress or places that person in reasonable apprehension of immediate or future bodily harm, sexual assault, confinement, or restraint.
        i. Anonymously or by name uses an electronic communications device to:
            1. Threaten the person who receives the communication.
            2. Create a page on a commercial social networking site or other Internet website.

3. Post or send one or more messages on or through a commercial social networking site or other Internet website, other than on or through an electronic mail program or message board program.
4. Send an electronic mail, instant message, text message, or similar communication.

b. Without lawful authority engages in the use of an electronic communications device to hinder, stop or invade the online activity of another which would result in a reasonable person becoming terrified, intimidated, threatened, harassed, suffer serious emotional distress or places that person in reasonable apprehension of immediate or future bodily harm, sexual assault, confinement, or restraint.
    i. This activity incudes, but is not limited, to:
        1. The transmission of program information, code, or command resulting in a machine or network resource becoming unavailable to its intended users by temporarily or indefinitely interrupting or suspending the services of a host connected to the Internet.
        2. The transmission of program information, code, or command resulting in the release of information that references a name, domain address, phone number, or other item of information a reasonable person would consider private, belonging to any person without obtaining the person's consent.

c. Without lawful authority, on at least two separate occasions, engages in online impersonation.
    i. Without obtaining a person's consent using the name or persona of that

person to:

1. Create a page on a commercial social networking site or other Internet website.
2. Post or send one or more messages on or through a commercial social networking site or other Internet website, other than on or through an electronic mail program or message board program.
3. Send an electronic mail, instant message, text message, or similar communication that references a name, domain address, phone number, or other item of identifying information belonging to any person without obtaining the person's consent.

d. Without lawful authority on two or more occasions engages in unlawful surveillance by means of any electronic, digital or global positioning system device, surveillance technologies, or any other electronic communications device to determine a person's exact location, or determine a person's Internet or wireless activity without the consent of the individual.

e. Without lawful authority elicits or engages in repeated telephone calls or repeated contact either themselves or from third parties by means of an electronic communications device, or elicits or makes any combination of calls or contact, whether or not conversation ensues, in which a reasonable person would be terrified, intimidated, threatened, harassed, suffer serious emotional distress or places that person in reasonable apprehension of immediate or future bodily harm, sexual assault, confinement, or restraint.

f. Without lawful authority engages in conduct by means of an electronic

communications device, commercial social networking site or other Internet website, that arranges, specifically requests, or intentionally causes another person to engage in all mentioned behavior, which would result in a reasonable person becoming terrified, intimidated, threatened, harassed, or suffer serious emotional distress or places that person in reasonable apprehension of immediate or future bodily harm, sexual assault, confinement, or restraint.

g. This section does not apply to constitutionally protected speech or activity or to any other activity authorized by law.

II. Nonconsensual Pornography. A person commits nonconsensual pornography by intentionally, knowingly, recklessly, or with criminal negligence doing any of the following:

a. Without lawful authority distributes or posts by means of an electronic communications device the image of the intimate body part, body parts, or nude figure of another identifiable individual, or an image of the person depicted engaged in an act of sexual intercourse, sodomy, oral copulation, sexual penetration, or an image of masturbation by the person depicted or in which the person depicted participates, which would result in a reasonable person becoming terrified, intimidated, threatened, harassed, suffer serious emotional distress or places that person in reasonable apprehension of immediate or future bodily harm, sexual assault, confinement, or restraint.

i. The image, whether originally obtained with or without the consent of the individual depicted is distributed without consent from the individual depicted.

b. Without lawful authority distributes or posts by means of an electronic communications device, commercial social networking site or other Internet website the sexually explicit or nude images of an individual accompanied by the the release of information that references a name, domain address, phone number, or other item of information a reasonable person would consider private, belonging to the depicted individual, which would result in a reasonable person becoming terrified, intimidated, threatened, harassed, or suffer serious emotional distress or places that of that person in reasonable apprehension of immediate or future bodily harm, sexual assault, confinement, or restraint. .

    1. Distributes on a commercial social networking site or other Internet website, electronic mail, instant message, text message, or similar communication that references a name, domain address, phone number, or other item of identifying information belonging to any person without obtaining the person's consent.

c. Without lawful authority distributes or posts by means of an electronic communications device, commercial social networking site or other Internet website, or arranges, specifically requests, or intentionally causes another person to distribute that image or video, which would result in a reasonable person becoming terrified, intimidated, threatened, harassed, suffer serious emotional distress or places that person in reasonable apprehension of immediate or future bodily harm, sexual assault, confinement, or restraint.

d. All images depicting the intimate body part, body parts, or nude figure of another identifiable individual, or an image of the individual engaged in an act of sexual

intercourse, sodomy, oral copulation, sexual penetration, or an image of masturbation by the person depicted or in which the person depicted participates, is deemed private unless specifically stated otherwise by the depicted individual.

e. This section does not apply to constitutionally protected speech or activity or to any other activity authorized by law:
    i. The distribution is made in the course of reporting an unlawful activity.
    ii. The distribution is made by a law enforcement official in connection with a criminal prosecution.
    iii. The distribution is made by a person acting in compliance with a subpoena or court order for use in a legal proceeding.
    iv. The distribution is made by a person acting with a bona fide and lawful scientific, educational, governmental, news, or other similar public purpose.
    v. The image is of a voluntary exposure in a public or commercial setting.
    vi. The distribution is made in the course of a lawful public proceeding.

III. Threats of Sexual Violence. A person commits threats of sexual violence by intentionally, knowingly, recklessly, or with criminal negligence doing any of the following:

a. Without lawful authority directs any obscene, lewd profane, or threatening language or suggests or threatens any lewd or violent act to an individual by means of an electronic communications device which would result in a reasonable person becoming terrified, intimidated, threatened, harassed, or suffer serious emotional distress or places that person in reasonable apprehension of immediate or future bodily harm, sexual assault, confinement, or restraint.

b. Without lawful authority creates and/or distributes photos, videos, games, or other visual forms of communication by means of an electronic communications device that depicts an individual as a victim of sexual violence, which would result in a reasonable person becoming terrified, intimidated, threatened, harassed, suffer serious emotional distress or places that person in reasonable apprehension of immediate or future bodily harm, sexual assault, confinement, or restraint.

c. This section does not apply to constitutionally protected speech or activity or to any other activity authorized by law.

IV. Online Sexual Coercion. A person commits online sexual extortion by intentionally, knowingly, recklessly, or with criminal negligence doing any of the following:

a. Without lawful authority threatens to distribute by means of an electronic communications device, commercial social networking site or other Internet website the sexually voyeuristic, explicit or nude images of an individual obtained with or without their consent in order to obtain an item or service, which would result in a reasonable person becoming terrified, intimidated, threatened, harassed, suffer serious emotional distress, or places that person in reasonable apprehension of immediate or future bodily harm, sexual assault, confinement, or restraint.

V. Digital Voyeurism. A person commits digital voyeurism by intentionally, knowingly, recklessly, or with criminal negligence doing any of the following:

a. Without lawful authority records by means of an electronic communications device sexually voyeuristic or explicit images of an individual without obtaining their consent, in which a reasonable person would be terrified, intimidated, threatened, harassed, or suffer serious emotional distress.

b. Without lawful authority distributes or posts by means of an electronic communications device, commercial social networking site or other Internet website the sexually voyeuristic or explicit images of an individual without obtaining their consent, which would result in a reasonable person becoming terrified, intimidated, threatened, harassed, or suffer serious emotional distress.

VI. Cyberbullying. A person commits cyberbullying by intentionally, knowingly, recklessly, or with criminal negligence doing any of the following:

a. Transmits, sends or posts a malicious communication or engages in malicious conduct directed at a specific person by means of an electronic communications device, commercial social networking site or other Internet website, which would result in a reasonable person of a similar disposition to feel alarmed, harassed, intimidated, terrified, or threatened, or face substantial emotional, psychological, or physical harm.

i. Psychological harm includes but is not limited to psychiatric admission or suicide.

b. The transmission was in furtherance of severe, repeated, or hostile behavior.

c. Both the sender and recipient of the communications are under the age of eighteen years old.

d. This section does not apply to constitutionally protected speech or activity or to any other activity authorized by law.

VII. Penalties

a. Cyberstalking is a felony:

i. Cyberstalking is a class [ ] felony if committed intentionally

ii. Cyberstalking is a class [ ] felony if committed knowingly

iii. Cyberstalking is a class [ ] felony if committed recklessly

iv. Cyberstalking is a class [ ] felony if committed with criminal negligence

1. Punishment gradually decreases from intentional to criminal negligence

b. Nonconsensual Pornography is a felony:

i. Nonconsensual Pornography is a class [ ] felony if committed intentionally

ii. Nonconsensual Pornography is a class [ ] felony if committed knowingly

iii. Nonconsensual Pornography is a class [ ] felony if committed recklessly

iv. Nonconsensual Pornography is a class [ ] misdemeanor if committed with criminal negligence

1. Punishment gradually decreases from intentional to criminal negligence

c. Threats of Sexual Violence is a felony:

i. Threats of Sexual Violence is a class [ ] felony if committed intentionally

ii. Threats of Sexual Violence is a class [ ] felony if committed knowingly

iii. Threats of Sexual Violence is a class [ ] felony if committed recklessly

iv. Threats of Sexual Violence is a class [ ] misdemeanor if committed with criminal negligence

1. Punishment gradually decreases from intentional to criminal negligence

d. Online Sexual Coercion is a felony:

i. Online Sexual Extortion is a class [ ] felony if committed intentionally

ii. Online Sexual Extortion is a class [ ] felony if committed knowingly

iii. Online Sexual Extortion is a class [ ] felony if committed recklessly

iv. Online Sexual Extortion is a class [ ] felony if committed with criminal negligence

1. Punishment gradually decreases from intentional to criminal negligence

e. Digital Voyeurism is a misdemeanor:

i. Digital Voyeurism is a class [ ] misdemeanor if committed intentionally

ii. Digital Voyeurism is a class [ ] misdemeanor if committed knowingly

iii. Digital Voyeurism is a class [ ] misdemeanor if committed recklessly

iv. Digital Voyeurism is a class [ ] misdemeanor if committed with criminal negligence

1. Punishment gradually decreases from intentional to criminal negligence

f. Cyberbullying is a misdemeanor:

i. Cyberbullying is a class [ ] misdemeanor if committed intentionally

ii. Cyberbullying is a class [ ] misdemeanor if committed knowingly

iii. Cyberbullying is a class [ ] misdemeanor if committed recklessly

iv. Cyberbullying is a class [ ] misdemeanor if committed with criminal negligence

1. Punishment gradually decreases from intentional to criminal negligence

VIII. Jurisdiction. Any offense under this article committed by the use of an electronic communications or by electronic communication device may be deemed to have been committed:

a. Where the electronic communication was originally sent or where it was originally received in this state.

b. Where the offense was committed either wholly or partly within this state.

c. Where an element of the offense was committed in this state.

d. Where the offense was committed outside this state and resulted in harm to a person in this state.

IX. Definitions:

a. “Cyberbullying” is the repeated transmission of any electronic textual, visual, written, or oral communication to coerce, abuse, torment, or intimidate a person under the age of eighteen by another underage individual.

b. “Cyberstalking” includes the repeated pursuit of a person by one or more individuals that involves the repeated threats and/or harassment by the use of electronic mail or other computer-based communication that would make a reasonable person afraid or concerned for their safety. This comprises both emotional and behavioral components, where the victim is harmed by constant suffering stemming from fear.

c. "Conduct" includes any communications, made by means of an electronic communication device, that is so unequivocal, unconditional, immediate, and specific as to convey a gravity of purpose and a prospect of execution, even if there is no intent of actually engaging in the conduct, and as a result a reasonable

person would fear for his or her safety or the safety of his or her family.

d. “Digital voyeurism” entails instances of surreptitiously taken images of an individual’s private areas, albeit clothed, with the purpose of sexual gratification.

e. "Electronic communication" means any transfer of signs, signals writings, sounds, data, photographs, or intelligence of any nature transmitted in whole or in part by an electronic communications device. It includes, but is not limited to, e-mail, Internet-based communications, instant message, text message, or voice mail.

f. "Electronic communications device" includes, but is not limited to: wire, radio, electromagnetic, photoelectric, and photo-optical systems including online communications, telephones, cellular telephones, computers, video recorders, fax machines, or pagers.

g. "Emotional distress" means significant mental suffering, anxiety, or alarm.

h. "Harm" includes loss of employment, economic injuries, emotional distress, deterioration of victim’s physical and mental health, physical harm or harassment by third-party individuals, and online or offline stalking.

i. "Harass" means to engage in conduct directed toward a person that alarms, torments, or terrorizes that person.

j. “Image” includes a photograph, film, videotape, digital reproduction, or other reproduction.

k. “Intimate body part” means any portion of the genitals, the anus and in the case of a female, also includes any portion of the breasts below the top of the areola, that is either uncovered or clearly visible through clothing. “Nude” means that no article of clothing is present on the body of the individual depicted, which allows

any “intimate body part” to be seen.

l. “Nonconsensual/revenge pornography” means a form of sexual assault involving the unauthorized distribution on the Internet of intimate images of a nude individual posing or engaging in various sexual activities. This includes images obtained without consent (e.g., hidden recordings or recordings of sexual assaults) as well as images.

m. “Online sexual coercion” entails the use of various means available online to elicit sexual cooperation by putting some kind of pressure on a victim that is enacted through trickery, blackmail, and includes the obtainment of extortion materials through either legal or illegal means.

n. “Sexual act” includes contact, whether using a body part or other object, with a person’s genitals, anus or a female adult nipple for the purposes of sexual gratification.

o. “Surveillance technology/technologies” includes but is not limited to hidden mobile apps, GPS tracking, webcam hacking, and more advanced techniques like traffic analysis, spyware, key loggers, backdoors, viruses, and Trojans.

p. “Unlawful surveillance” means the repeated act of recording, monitoring, or observing information, such as activities and behavior, for purposes of gathering personal data regarding an individual or group of individuals.

V. Conclusion

Online gendered harassment and violence is a growing phenomenon within online communities. By attacking individuals for their gender, OGHV sexualizes, threatens, and discriminates against women. Such behavior not only causes severe emotional, mental, and physical harm for victims, but also has a detrimental impact on both online and offline societies.

Major Findings

There are a number of reasons as to why OGHV has yet to be adequately addressed in state and federal legislature. The unique characteristics of online communication, including anonymity, cyber mobs, and the perpetuity of harm, victimize in new ways that increases the harm's severity, and sets OGHV apart from gendered crimes perpetrated offline. These characteristics give the offender advantages over both victims and law enforcement, as they can mask their identity, proposition the help of thousands of individuals, and prolong the victim's harm years after the initial abuse. Trivialization of OGHV has also attempted to normalize OGHV behavior as courts, authorities and commentators claim it is harmless, avoidable, natural or a protected right of the abusers.

Such dismissal has stemmed reformation of outdated laws, many of which fail to address the unique aspects of OGHV crimes and the Internet itself. Civil torts of defamation and IIED that victims are advised to turn to do little to address the behavior or its harms. Either the offender's abuse is not encompassed under the tort, or precedent has concluded that the woman's suffering does not qualify as severe harm under the law. Victims' handling of the abuse themselves also costs time and money, which many victims may not have. Criminal requirements of credible threat and intent—originally crafted for offline harm—have failed to evolve along with current technology, leaving victims with no way to prove that offenders'

actions and threats have put them in fear for their safety. Unequal protection across state lines, current jurisdictional boundaries, and lack of police training on cyber and OGHV crimes have also created more hurdles for authorities and victims to overcome than helping to redress suffering.

To rectify this, legislation must be updated, specifically focusing on stricter implementation of criminal punishment, amending current Internet law, and educating the public through new policies. The different forms of OGHV must be clearly defined, with special attention paid to how the harms are delivered and what they constitute. Lowering the culpable mental state, expanding the definition of digitally communicated threats, and extending jurisdictional reach of OGHV crimes will close loopholes that offenders commonly use to escape prosecution. The more subjective line of inquiry will also do more to recognize victims' suffering and redress it accordingly. Revising Section 230 of the CDA will also exclude those websites whose purpose is to cause harm, while providing guidelines for websites and ISPs to follow to ensure best practices while protecting users' rights. Providing education and training policies for schools, businesses, and law enforcement will also change the current cultural perception of OGHV, and help to prevent and stop future occurrences and harm.

Limitations of the Study

One of the major limitations in past studies is the combination of behaviors when gathering data. Methodological issues in measuring cyberstalking commonly combined instances of online sexual harassment. While these behaviors can be enacted together, research on the them as separate entities would have provided more accurate data. Current data is also limited due to OGHV being underreported. This may be because cases remain unsolved, victims are afraid to come forward, or inaccurate reporting by police departments. Problems may also arise due to the

inconsistency of state definitions of OGHV, as the same behaviors may be reported differently across states or not reported at all.

While the examples of OGHV used within this study did well in showing the behaviors' harms, examples heard first-hand would have been preferred. As this study did not interview victims directly, reliance on the accuracy of second-hand sources, such as magazines and newspapers, was necessary. While this study was thorough in checking sources reliability, there is a possibility that some organizations embellished, skewed, or misreported facts of the case. Interviews with the victims directly would have accounted for possible inaccuracies in reporting, and might have provided better insight into victims' experiences.

The infancy of cyber rape also provided limitations. While cyber rape is included in the OGHV framework, little research has been conducted on the topic to provide useful insights. Much like the other behaviors, cyber rape also has no scientifically agreed-upon definition in the research community. For these reasons, there are not many reliable statistics and data available in the field of cyber rape. This limited understanding of the behavior, its effects, and thus the possible solutions to the problem that could be proposed, hindered its inclusion in this study.

Recommendations for Future Research

Many states currently do not have a unified definition of different OGHV behaviors, with punishments for perpetrators ranging in severity. This creates unequal protection for victims, and creates barriers for police and prosecutors. To better provide equal and comprehensive protection to all citizens, states should consider revising their current laws to better encompass the unique aspects of Internet communication and OGHV. This study proposed suggestions as one such option of reform. However, as technology and communication changes, lawmakers should pay attention to its new forms and adapt their laws accordingly to ensure citizens future protection.

Mandatory training for police should also be implemented to ensure that officers are adequately prepared on how to deal with these cyber crimes, and ensure victims' complaints are taken seriously. Employers should be educated on OGHV, and policies should be enacted to ensure that victims are not barred from economic opportunities based on searches that reveal their online abuse. School faculty should also be better trained and equipped for dealing with instances of gendered cyberbullying—and bullying as a whole—to ensure action by the administration. Requiring school faculty to submit reports on cyberbullying cases and how they were addressed would also provide more data for researchers and authorities on how best to approach different cases. Education on OGHV should also be added to school curriculums to teach students about the behaviors and their harms, with the goal of stopping current cyberbullying and preventing future OGHV behavior.

Academic literature and research must be updated to account for these new forms of gender discrimination. While many researchers have already investigated different forms of OGHV, attention must be paid to gathering data on the behaviors as *separate* entities in conjunction with their combined occurrence. This will provide better data on how the communications are being carried out, what they entail, and their effects on specific groups. Further research into how OGHV may affect other minority groups, such as the LGBTQ community, may also be conducted to better understand the harms on those specific populations. Due to the limited data on cyber rape, future research should focus on the behavior to garner a better understanding of where it occurs, who perpetrates it, the harms, and possible ways to hinder it if necessary. More research into how civil laws may be updated to encompass less severe forms of OGHV should also be followed.

The Internet is a medium filled with pleasures and vices. Much like offline contact, there will always be those communications that are insulting, degrading, and against public sensibilities, but protected as free speech. However, by naming the worst forms of OGHV as criminal and implementing updated laws and policies to account for its unique characteristics, online harm can be re-characterized to reveal its serious nature. The United States can benefit from looking at its past criminalization of offline gendered harms, and use the knowledge of its failures and successes to create effective OGHV statutes. Recommendations have been made in order to create effective law that can better protect victims and prosecute offenders, and thus spur significant changes to online behavior.

Definitions

- *Anonymity/Anonymous*- Having an unknown or unacknowledged name; Having an unknown or withheld authorship or agency; Having no distinctive character or recognition factor
- *Click wrap*- Agreements formed on the Internet. A website provider generally posts terms and conditions and the user clicks an "I Accept" button. The courts have generally held these agreements to be enforceable
- *Civil Tort*- civil wrongs recognized by law as grounds for a lawsuit. These wrongs result in an injury or harm constituting the basis for a claim by the injured party. While some torts are also crimes punishable with imprisonment, the primary aim of tort law is to provide relief for the damages incurred and deter others from committing the same harms.
- *Contributory Copyright Infringement*- an individual knowingly induces, causes or materially contributes to copyright infringement, but who has not committed or participated in the infringing acts themselves. The individuals may be held liable as a contributory infringer if he or she had knowledge, or reason to know, of the infringement
- *Cyberbullying*- The repeated transmission of any electronic textual, visual, written, or oral communication to coerce, abuse, torment, or intimidate a person under the age of eighteen by another underage individual.
- *Cyber Mobs*- when people join together, usually anonymously, to humiliate or manipulate a chosen target via the Internet.
- *Cyber Rape*- The act of forced online sexual activity (i.e. rape or sexual assault) whether through text, animation, malicious scripts or other means where one of the two people does not want the sexually oriented messages.
- *Cyberstalking*- the repeated pursuit of a person by one or more individuals that involves

repeated threats and/or harassment by the use of electronic mail or other computer-based communication that would make a reasonable person afraid or concerned for their safety. This comprises both emotional and behavioral components, where the victim is harmed by constant suffering stemming from fear.

- *Defamation Tort*- Defamation is a statement that injures a third party's reputation. The tort of defamation includes both libel (written statements) and slander (spoken statements).
- *Deindividuation*- the loss of self-awareness in groups
- *Denial of Service Attack (DoS)*- an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet
- *Denigration*- harmful, untrue, or cruel statements about a person to other people or posting such material online
- *Distributed Denial of Service attack (DDoS)*- occurs when multiple systems flood the bandwidth or resources of a targeted system, usually with one or more web servers and unique IP addresses.
- *Digital Sexual Coercion (Sextortion)*- entails the use of various means available online to elicit sexual cooperation by putting some kind of pressure on a victim that is enacted through trickery, blackmail, and includes the obtainment of extortion materials through either legal or illegal means.
- *Digital Voyeurism ("Creepshots")*- entails instances of surreptitiously taken photos or videos of an individual's clothed private areas with the purpose of sexual gratification.
- *Electronic Communication*-any transfer of signs, signals writings, sounds, data, photographs, or intelligence of any nature transmitted in whole or in part by an electronic communications

device. It includes, but is not limited to, e-mail, Internet-based communications, instant message, text message, or voice mail.

- *Electronic Communications Device*-includes, but is not limited to: wire, radio, electromagnetic, photoelectric, and photo-optical systems including online communications, telephones, cellular telephones, computers, video recorders, fax machines, or pagers.
- *Emotional Distress*- significant mental suffering, anxiety, or alarm
- *Exclusion*- maliciously excluding someone from an online group
- *Flaming*- the sending of angry, rude, vulgar messages about a person to an online group or the person's electronic mail
- *Gendered Harassment (online)*- Set of three core features: 1) it's victims belong to historically subordinate groups (i.e. females), 2) the harassment is aimed at particular individuals personally and by name, and 3) the graphic, vicious and public abuse invokes the targeted individual's gender in threatening and degrading ways that interfere with individual's livelihoods and education. Online Sexual Harassment is a subsection.
- *Google Bombing*- practice whereby a specific web page is targeted to rank in 1st position in the SERPs for a particular search phrase, so that when that phrase is typed in Google it brings specific, and usually controversial, results.
- *Harm*- includes loss of employment, economic injuries, emotional distress, deterioration of victim's physical and mental health, physical harm or harassment by third-party individuals, and online or offline stalking
- *Harass*-means to engage in conduct directed toward a person that alarms, torments, or terrorizes that person.
- *Intent*- refers to the state of mind with which the act is done or committed.

- *General Intent*- the intent to do that which the law prohibits—it is not necessary for the prosecution to prove that the defendant intended the precise harm or the precise result that occurred.
- *Specific Intent*- a particular state of mind that seeks to accomplish the precise act that the law prohibits—the prosecution must show that the defendant purposely or knowingly caused the harm at issue.

- *Intimate Body Part*- any portion of the genitals, the anus and in the case of a female, also includes any portion of the breasts below the top of the areola, that is either uncovered or clearly visible through clothing. "Nude" means that no article of clothing is present on the body of the individual depicted, which allows any "intimate body part" to be seen.
- *Internet Protocol address (IP address)*- the numerical label assigned to each device (e.g., computer) participating in a computer network
- *Jailbait*- a person who is younger than the legal age of consent for sexual activity, with the implication that a person above the age of consent might find them sexually attractive; a girl with whom sexual intercourse is punishable as statutory rape because she is under the legal age of consent.
- *Masquerade*- perpetrators pretend to be someone else and send or post material that makes the victim look bad
- *Nonconsensual/Revenge Pornography*- The unconsented distribution of an of the intimate body part, body parts, or nude figure of another identifiable individual, or an image of the person depicted engaged in an act of sexual intercourse, sodomy, oral copulation, sexual penetration, or an image of masturbation by the person depicted or in which the person

depicted participates, under circumstances in which the persons agree or understand that the image shall remain private.

- *Online Disinhibition Effect*- a loosening (or complete abandonment) of social restrictions and inhibitions that would otherwise be present in normal face-to-face interaction during interactions with others on the Internet.
- *Online Gendered Harassment and Violence (OGHV)*- Describes collectively the range of criminal, civil, and collective harm caused by aggressive behaviors perpetrated against individuals due to and with specific focus on their gender with the aid or use of cyberspace. Categorize this through 4 different behaviors
    - Cyberbullying
    - Online Sexual Harassment
    - Cyberstalking
    - Cyber Rape
- *Online Sexual Coercion ("Sextortion")*- the use of various means available online to elicit sexual cooperation by putting some kind of pressure on a victim
- *Online Sexual Harassment*- unwelcomed verbal or graphic conduct of a sexual nature that creates a hostile or offensive environment online.
    - Verbal online sexual harassment- offensive sexual messages actively initiated by one or more perpetrators towards the victim
    - Graphic online sexual harassment- the intentional sending of erotic and pornographic images through either individual online communication channels, such as e-mail, or posting them on online forums

- *Outings*- the sending or posting material about a person that contains sensitive, private or embarrassing information, including forwarding private messages or images
- *Selfie*- a self-portrait photograph, typically taken with a digital camera or camera phone held in the hand or supported by a selfie stick
- *Spiral of Silence*- fear of isolation from a group due to one's opinion which consequently leads to remaining silent instead of voicing opinions.
- *Streisand Effect*- the phenomenon whereby an attempt to hide, remove, or censor a piece of information has the unintended consequence of publicizing the information more widely
- *Swatting*- the act of deceiving an emergency service—via such means as hoaxing an emergency services dispatcher—into dispatching an emergency response based on the false report of an ongoing critical incident.
- *Third Party Stalkers*- a type of stalking by proxy where the perpetrator incites others to engage in harassing activities on his/her behalf. This may include activities such as placing false advertisements on the Internet using the victim's contact details
- "*Troll*"- One who posts a deliberately provocative message to a newsgroup or message board with the intention of causing maximum disruption and argument; someone who leaves an intentionally annoying message on the Internet, in order to get attention or cause trouble
- *Trolling*- to post inflammatory or inappropriate messages or comments on the Internet, especially a message board, for the purpose of upsetting other users and provoking a response
- *Unlawful Surveillance*- the repeated act of recording, monitoring, or observing information, such as activities and behavior, for purposes of gathering personal data regarding an individual or group of individuals

References

17 U.S.C. *§* 512- *Digital Millennium Copyright Act.* (2010).

18 U.S. Code § 2261A – Stalking. (2013).

18 U.S. Code § 875 - Interstate communications. (1994).

47 U.S. Code § 230 - Protection for private blocking and screening of offensive material. (1998).

47 U.S. Code § 223 - Obscene or harassing telephone calls in the District of Columbia or in interstate or foreign communications. (2013).

720 ILL. COMP. STAT. 5/12-7.5- Intimidation. (2012).

Abril, P. S. (2007). Recasting privacy torts in a spaceless world. *Harvard Journal of Law and Technology*, 21 (1), 1–47. Retrieved from http://jolt.law.harvard.edu/articles/pdf/v21/21HarvJLTech001.pdf

Adkins, L. (1999). Community and economy: A retraditionalization of gender? *Theory, Culture & Society, 16*(1), 119-139. Retrieved from http://search.proquest.com/docview/61485743?accountid=14667

Ahlgrim, B. J. M. (2015). *Cyber stalking: Impact of gender, cyber stalker-victim relationship and proximity* (Order No. 1594405). . (1700356585). Retrieved from http://search.proquest.com/docview/1700356585?accountid=35396

Ajmani, N. (2011). Cyberstalking and free speech: rethinking the Rangel standard in the age of the Internet. *Oregon Law Review*, *90*(1), 303-334. Retrieved from https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/11760/Ajmani.pdf?seq

uence=1&isAllowed=y

alienth. (2014). Time to talk: announcements. Retrieved from https://www.reddit.com/r/announcements/comments/2fpdax/%20time_to_talk/

AR Code § 5-71-217. (2012).

Bamford, A. (2004). Cyber-Bullying. *AHISA Pastoral Care National Conference. Melbourne, Australia.* Retrieved from http://www.darrenarcher.name/year10/PDFs/ahisaconference-bamfordcyberbullying.pdf

Barak, A. (2005). Sexual harassment on the Internet. *Social Science Computer Review*, *23*(1), 77-92. doi:10.1177/0894439304271540

Baum, K., & Rose, K. (2009). *National crime victimization survey: stalking victimization in the United States*. Retrieved from Bureau of Justice Statistics website: https://www.victimsofcrime.org/docs/src/baum-k-catalano-s-rand-m-rose-k-2009.pdf?sfvrsn=0

Benfer, A. (2001, July 3). Cyber slammed. *Salon*. Retrieved from http://www.salon.com/2001/07/03/cyber_bullies/

Beran, T., & Li, Q. (2007). The relationship between cyberbullying and school bullying. *Journal of Student Wellbeing, 1(12),* 15-33. Retrieved from http://www.ojs.unisa.edu.au/index.php/JSW/article/viewFile/172/139

Blankstein, A. (2013, September 26). FBI arrests suspect in Miss Teen USA 'sextortion' case. *NBC News*. Retrieved from http://www.nbcnews.com/news/other/fbi-arrests-suspect-miss-teen-usa-sextortion-case-f8C11267183

Botelho, G. (2013, September 27). Arrest made in Miss Teen USA Cassidy Wolf 'sextortion' case. *CNN*. Retrieved from http://www.cnn.com/2013/09/26/justice/miss-teen-usa-sextortion/

Brandom, R. (2013, July 27). New £10 note gives rise to rape threats and anti-Twitter campaign. *The Verge*. Retrieved from http://www.theverge.com/2013/7/27/4563246/new-british-banknote-gives-rise-to-rape-threats-and-anti-twitter

Brenner, S. W., & Koops, B. (2004). Approaches to cybercrime jurisdiction. *Journal of High Technology Law*, *4*(1), 1-46. Retrieved from http://ssrn.com/abstract=786507

Cal. Penal Code, Title 15, *§*647. (2014).

Campbell, Marilyn A. (2005) Cyber bullying: An old problem in a new guise?. *Australian Journal of Guidance and Counselling* 15(1):68-76. Retrieved from http://eprints.qut.edu.au/1925/

Cecil, A. L. (2014). Taking back the internet: Imposing civil liability on interactive computer services in an attempt to provide an adequate remedy to victims of nonconsensual pornography. *Washington and Lee Law Review, 71*(4), 2512-2556. Retrieved from http://search.proquest.com/docview/1646465751?accountid=14667

Chen, A. (2012, October 12). Unmasking Reddit's Violentacrez, the biggest troll on the web. *Gawker*. Retrieved from http://gawker.com/5950981/unmasking-reddits-violentacrez-the-biggest-troll-on-the-web

Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. *Wake Forest Law Review*, *49*, 345-391. Retrieved from http://ssrn.com/abstract=2368946

Citron, D. K. (2014). *Hate crimes in cyberspace* (1st ed.). Cambridge, MA: Harvard University Press.

Citron, D. K. (2008). Cyber Civil Rights. *Boston University Law Review*, Vol. 89, pp. 61-125. Retrieved from http://ssrn.com/abstract=1271900

Citron, D. K. (2009). Law's expressive value in combating cyber gender harassment. *Michigan Law Review, 108*(3), 373-415. Retrieved from http://search.proquest.com/docview/201129725?accountid=14667

Civil Rights Act of 1964 (Pub. L. 88-352) (Title VII)

Cohen v. Google, 25 Misc. 3d 945, 946, n. 1 (N.Y. Sup. Ct. 2009)

Cox, C. (2014). Protecting victims of cyberstalking, cyberharassment, and online impersonation through prosecutions and effective laws. *Jurimetrics, 54*(3), 277-302. Retrieved from http://search.proquest.com/docview/1541971986?accountid=14667

Cyber Civil Rights Initiative. (n.d.). 27 states have revenge porn laws. Retrieved April 14, 2016, from http://www.cybercivilrights.org/revenge-porn-laws/

Dahl, J. (2014, March 18). Do police take online threats against women seriously? *CBS News* [New York]. Retrieved from http://www.cbsnews.com/news/do-police-take-online-threats-against-women-seriously/

Deirmenjian, J. M. (1999). Stalking in cyberspace. *Journal of American Academic Psychiatry Law*, *27*, 407-413. Retrieved from http://www.jaapl.org/content/27/3/407.full.pdf+html

Digital Millennium Copyright Act of 1998 (Pub. L. 105–304) (1998)

D'Ovidio, R., & Doyle, J. (2003). Study on Cyberstalking Understanding Investigative Hurdles, A. *FBI Law Enforcement Bulletin*, *27*(3), 3.

Doll, J. (2012, November 27). Welcome to the twisted age of the Twitter death threat. *The Wire*. Retrieved from http://www.thewire.com/technology/2012/11/welcome-twisted-age-twitter-death-threat/59354/

Duggan, M., Rainie, L., Smith, A., Funk, C., Lenhart, A., & Madden, M. (2014). *Online harassment*. Retrieved from Pew Research Center website: http://www.pewinternet.org/2014/10/22/online-harassment/?beta=true&utm_expid=53098246-2.Lly4CFSVQG2lphsg-KopIg.1

Edgington, N. (2012, February). The girl who got even: A true cyberbullying story. *Choices*. Retrieved from http://choices.scholastic.com/story/girl-who-got-even-true-cyberbullying-story

Electronic Frontier Foundation. (n.d.). CDA 230: The most important law protecting Internet speech. Retrieved from https://www.eff.org/issues/cda230

Elonis v. United States, No.13-983 575 U.S. ___ (2015)

Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008)

Finkel v. Dauber, 29 Misc.3d 325 (N.Y. Misc., 2010)

Fitzpatrick, D., & Griffen, D. (2012, October 19). Man behind 'Jailbait' posts exposed, loses job. *CNN*. Retrieved from http://www.cnn.com/2012/10/18/us/internet-troll-apology/

Franks, M. A. (2012). Sexual harassment 2.0. *Maryland Law Review*, *71*(3), 655-704. Retrieved from http://ssrn.com/abstract=1492433

Franks, M. A. (2011). Unwilling avatars: idealism and discrimination in cyberspace. *Columbia Journal of Gender and Law*, *20*(2), 224-249. Retrieved from http://ssrn.com/abstract=1374533

Freiberger, K. L. (2008). *Examining incidents of cyberstalking: An exploration of an emerging crime* (Order No. 3316846). Available from ProQuest Dissertations & Theses A&I; ProQuest Dissertations & Theses Global. (304841187). Retrieved from http://search.proquest.com/docview/304841187?accountid=14667

Fusco, C. A. (2014). *Stalking 2.0: The era of cyberstalking* (Order No. 1571120). Available from ProQuest Dissertations & Theses A&I; ProQuest Dissertations & Theses Global. (1641123312). Retrieved from http://search.proquest.com/docview/1641123312?accountid=14667

Geare, A. J. (1998). Sexual harassment: Modern issue--ancient problem. *New Zealand Journal of Industrial Relations, 22/23*(3), 241-276. Retrieved from http://search.proquest.com/docview/213511841?accountid=14667

Genn, B. A. (2014). What comes off, comes back to burn: revenge pornography as the hot new flame and how it applies to the First Amendment and privacy law. *The American University Journal of Gender, Social Policy & the Law, 23*(1), 163-195. Retrieved from http://search.proquest.com/docview/1640728632?accountid=14667

Goodno, N.H. (2007). Cyber stalking, a new crime: Evaluating the effectiveness of current state and federal laws. *Missouri Law Review.* 72, 125 – 197. Retrieved from http://scholarship.law.missouri.edu/mlr/vol72/iss1/7

Greenberg, A. (2014, September 10). Hacked celeb pics made Reddit enough cash to run its

servers for a month. *Wired*. Retrieved from http://www.wired.com/2014/09/celeb-pics-reddit-gold/

Gumbus, A., & Meglich, P. (2013). Abusive online conduct: Discrimination and harassment in cyberspace. *Journal of Management Policy and Practice, 14*(5), 47-56. Retrieved from http://search.proquest.com/docview/1503083505?accountid=14667

Hall, D. M. (1997). *Outside looking in: Stalkers and their victims* (Order No. 9806419). Available from ProQuest Dissertations & Theses A&I; ProQuest Dissertations & Theses Full Text; ProQuest Dissertations & Theses Global. (304359004). Retrieved from http://search.proquest.com/docview/304359004?accountid=14667

Hattenstone, S. (2013, August 4). Caroline Criado-Perez: 'Twitter has enabled people to behave in a way they wouldn't face to face'. *The Guardian*. Retrieved from http://www.theguardian.com/lifeandstyle/2013/aug/04/caroline-criado-perez-twitter-rape-threats

Henry, N., & Powell, A. (2015). Embodied harms: Gender, shame, and technology-facilitated sexual violence. *Violence Against Women, 21*(6), 758. Retrieved from http://search.proquest.com/docview/1682905022?accountid=14667

Hess, A. (2014, January 6). Why women aren't welcome on the Internet. *Pacific Standard*. Retrieved from http://www.psmag.com/health-and-behavior/women-arent-welcome-internet-72170

Hess, A. (2015, February 20). Hunter Moore is probably going to prison. How scared should revenge porn kingpins be? *Slate*. Retrieved from http://www.slate.com/blogs/the_slatest/2015/02/20/hunter_moore_guilty_plea_reveng

e_porn_king_pleads_guilty_to_hacking_faces.html

Hinduja, S., & Patchin, J. W. (2016). *State cyberbullying laws- A brief review of state cyberbullying laws and policies*. Retrieved from Cyberbullying Research Center website: http://cyberbullying.org/Bullying-and-Cyberbullying-Laws.pdf

Jacobs, H. (2013, November 13). Being a victim of revenge porn forced me to change my name-now I'm an activist dedicated to helping other victims. *xoJane*. Retrieved from http://www.xojane.com/it-happened-to-me/revenge-porn-holly-jacobs

Jameson, S. (2008). Cyberharrasment: Striking a Balance between Free Speech and Privacy. *CommLaw Conspectus: Journal of Communications Law and Technology Policy*, *17*(1), 231-266. Retrieved from http://scholarship.law.edu/cgi/viewcontent.cgi?article=1403&context=commlaw

Jason, Z. (2015, May). Game of fear. *Boston Magazine*. Retrieved from http://www.bostonmagazine.com/news/article/2015/04/28/gamergate/

Jones, S. (2013, July 29). Labour MP Stella Creasy receives Twitter rape threats. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2013/jul/29/labour-mp-stella-creasy-twitter-rape-threats

Jones v. Dirty World Entertainment Recordings LLC, No. 13-5946 (6th Cir., 2014)

King, A. V. (2010). Constitutionality of cyberbullying laws: Keeping the online playground safe for both teens and free speech. *Vanderbilt Law Review, 63*(3), 845-884. Retrieved from http://search.proquest.com/docview/346157717?accountid=14667

King-Ries, A. (2011). Teens, technology, and cyber stalking: The domestic violence wave of the future? *Texas Journal of Women and the Law.* 20(2), 131 – 164. Retrieved from

http://www.longwood.edu/staff/miskecjm/400teenstech.pdf

LA Rev Stat § 14:40.7

Lee, P. Y. (2015, October 22). This is what being a woman online is like: "I will be hunting down a chick [who] looks as close as possible to you". *Salon*. Retrieved from http://www.salon.com/2015/10/22/this_is_what_being_a_woman_online_is_like_i_will_be_hunting_down_a_chick_who_looks_as_close_as_possible_to_you/

Lenhart, A. (2007). *Data memo*. Retrieved from Pew Internet & American Life Project website: http://www.pewinternet.org/2007/06/27/cyberbullying/

Levendowski, Amanda M. (2014). Using Copyright to Combat Revenge Porn Tri-State Region IP Workshop, Winter 2014; NYU Journal of Intellectual Property & Entertainment Law, Vol. 3, 2014. http://dx.doi.org/10.2139/ssrn.2374119

Lightburn, M. (2009). *Cyber bullying: A content analysis of existing literature* (Order No. 1466169). Available from ProQuest Dissertations & Theses Full Text; ProQuest Dissertations & Theses Global. (305181121). Retrieved from http://search.proquest.com/docview/305181121?accountid=14667

Liptak, A. (2015, June 1). Supreme Court overturns conviction in online threats case, citing intent. *The New York Times*. Retrieved from http://www.nytimes.com/2015/06/02/us/supreme-court-rules-in-anthony-elonis-online-threats-case.html?_r=0

Lithwick, D. (2007, May 4). Fear of blogging: why women shouldn't apologize for being afraid of threats on the Web. *Slate*. Retrieved from http://www.slate.com/articles/arts/culturebox/2007/05/fear_of_blogging.html

Luarn, P., & Hsieh, A. (2014). Speech or silence. *Online Information Review, 38*(7), 881. Retrieved from http://search.proquest.com/docview/1633961511?accountid=14667

Madden, M., Lenhart, A., Duggan, M., Cortesi, S., & Gasser, U. (2013). *Teens and Technology 2013*. Retrieved from Pew Research Center website: http://www.pewinternet.org/2013/03/13/teens-and-technology-2013/

MacKinnon, C. A. (1979). Legal context. In *Sexual harassment of working women: A case of sex discrimination* (pp. 101-142). New Haven: Yale University Press.

Madden, M., Lenhart, A., Duggan, M., Cortesi, S., & Gasser, U. (2013). *Teens and technology 2013*. Retrieved from Pew Research Center & The Berkman Center for Internet & Society at Harvard University website: http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_TeensandTechnology2013.pdf

Manuel, N. R. (2011). Cyber-bullying: Its recent emergence and needed legislation to protect adolescent victims. *Loyola Journal of Public Interest Law*, *13*, 219-252. Retrieved from http://heinonline.org/HOL/Page?handle=hein.journals/loyjpubil13&div=9&g_sent=1&collection=journals

Markey, L. M. (2013). *Starving the trolls: How the news media and harassment victims can fight harmful speech online* (Order No. 1539663). Retrieved from http://search.proquest.com/docview/1413302933?accountid=14667

Marwick, A. E., & Miller, R. (2014). *Online harassment, defamation, and hateful speech: A primer of the legal landscape*. Retrieved from Fordham Center on Law and Information website:

http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1002&context=clip

Massanari, A. (2015). #Gamergate and The Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures. *New Media & Society*, 1-18. Retrieved from http://nms.sagepub.com/content/early/2015/10/07/1461444815608807.full.pdf+html

McGrath, M. G., & Casey, E. (2002). Forensic psychiatry and the Internet: Practical perspectives on sexual predators and obsessional harassers in cyberspace. Journal of the American Academy of Psychiatry and the Law, 30(1), 81-94. Retrieved from http://www.jaapl.org/content/30/1/81.full.pdf+html

McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995)

Merlan, A. (2015, January 29). The cops don't care about violent online threats. What do we do now? *Jezebel*. Retrieved from http://jezebel.com/the-cops-dont-care-about-violent-online-threats-what-d-1682577343

Milford, T. S. (2013). *Girls' online agency: A cyberfeminist exploration* (Order No. MR95540). Available from ProQuest Dissertations & Theses Full Text; ProQuest Dissertations & Theses Global. (1473911165). Retrieved from http://search.proquest.com/docview/1473911165?accountid=14667

Miller, M. E. (2013, October 17). Revenge porn victim Holly Jacobs "ruined my life", ex says. *Miami New Times*. Retrieved from http://www.miaminewtimes.com/news/revenge-porn-victim-holly-jacobs-ruined-my-life-ex-says-6393654

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2001). *Risk factors for and impact of online sexual solicitation of youth*. Retrieved from http://unhinfo.unh.edu/ccrc/pdf/cv42jama.pdf

Nakashima, E. (2007, April 30). Sexual threats stifle some female bloggers. *The Washington*

Post. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2007/04/29/AR2007042901555.html?hpid=topnews

National Coalition Against Domestic Violence. (n.d.). What is domestic violence? Retrieved from http://www.ncadv.org/need-help/what-is-domestic-violence

New York Times Co. v. Sullivan, 376 U.S. 254 (1964)

O'Neill, B. (2011, November 7). The campaign to 'Stamp Out Misogyny Online' echoes Victorian efforts to protect women from coarse language. *The Telegraph*. Retrieved from http://blogs.telegraph.co.uk/news/brendanoneill2/100115868/the-campaign-to-stamp-out-misogyny-online-echoes-victorian-efforts-to-protect-women-from-coarse-language/

Owens, L., Shute, R., & Slee, P. (2000). Guess what I just heard: Indirect aggression among teenage girls in Australia. *Aggressive Behavior, 26,* 67-83. Retreived from https://www.researchgate.net/publication/228019267_Guess_what_I_just_heard%21_Indirect_aggression_among_teenage_girls_in_Australia._Aggressive_Behavior_26_67-83

Pagels, J. (2013, October 30). Death threats on Twitter are meaningless. You should ignore them. *Slate*. Retrieved from http://www.slate.com/blogs/future_tense/2013/10/30/twitter_death_threats_are_meaningless_you_should_ignore_them.html

Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the Schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice, 4(2),* 148-169. doi: 10.1177/1541204006286288

People v. Owens, 97 A.D.2d 855 (N.Y. App. Div. 1983)

Pittaro, M. L. (2007). Cyber stalking: An analysis of online harassment and intimidation. *International Journal of Cyber Criminology*, *1*(2), 180-197. Retrieved from http://www.cybercrimejournal.com/pittaroijccvol1is2.htm

Postmes, T., & Spears, R. (2002). Behavior Online: Does Anonymous Computer Communication Reduce Gender Inequality?. *Personality and Social Psychology Bulletin*, *28*(8), 1073-1083. doi:10.1177/01461672022811006

Quarmby, K. (2014, August 13). How the law is standing up to cyberstalking. *Newsweek*. Retrieved from http://www.newsweek.com/2014/08/22/how-law-standing-cyberstalking-264251.html

Rambo, K. S. (2003). *Trivial complaints: The role of privacy in domestic violence law and activism in the united states* (Order No. 3080353). Available from ProQuest Dissertations & Theses A&I; ProQuest Dissertations & Theses Full Text; ProQuest Dissertations & Theses Global. (288103547). Retrieved from http://search.proquest.com/docview/288103547?accountid=14667

Roberts, L. (2008). Jurisdictional and definitional concerns with computer-mediated interpersonal crimes: An analysis on cyber stalking. *International Journal of Cyber Criminology.* 2(1), 271 – 285. Retrieved from http://www.cybercrimejournal.com/lynnerobertsijccjan2008.pdf

Rockwood, M. (1977, April). Courts and cops: Enemies of battered wives. *Ms. Magazine*, 19.

Royse, A. (2008, August 3). Rape and death and Batman, OH MY! Retrieved from http://www.blogher.com/rape-and-death-and-batman-oh-my

Sandoval, G. (2013, September 12). The end of kindness: weev and the cult of angry young men. *The Verge*. Retrieved from http://www.theverge.com/2013/9/12/4693710/the-end-of-kindness-weev-and-the-cult-of-the-angry-young-man

Sarkeesian, A. (2012a, June 7). Feminist Frequency-Harassment, misogyny and silencing on YouTube. Retrieved from http://www.feministfrequency.com/2012/06/harassment-misogyny-and-silencing-on-youtube/

Sarkeesian, A. (2012b, June 10). Feminist Frequency-Harassment via Wikipedia vandalism. Retrieved from http://www.feministfrequency.com/2012/06/harassment-and-misogyny-via-wikipedia/

Sarkeesian, A. (2012c, July 1). Feminist Frequency-Image based harassment and visual misogyny. Retrieved from http://www.feministfrequency.com/2012/07/image-based-harassment-and-visual-misogyny/

Schwartz, K. E. (2009). Criminal liability for Internet culprits: the need for updated state laws covering the full spectrum of cyber victimization. *Washington University Law Review*, *87*(2), 407-436. Retrieved from http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1086&context=law_lawreview

Shariff, S., & Gouin, R. (2006). Cyber-dilemmas: Gendered hierarchies, new technologies and cyber-safety in schools. *Atlantis - A Women's Studies Journal*, 31 (1), 26-36. Retrieved from http://journals.msvu.ca/index.php/atlantis/article/viewFile/736/726

Shimizu, A. (2013). Recent developments: domestic violence in the digital age: towards the creation of a comprehensive cyberstalking statute. *Berkeley Journal of Gender, Law*

& Justice, *28*(1), 115-137. Retrieved from http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1315&context=bglj

Siddiqui, A. (1998). Sexual harassment law in America: Thirty years of evolution. *Asian Journal of Women's Studies, 4*(2), 87. Retrieved from http://search.proquest.com/docview/197716512?accountid=14667

Smith v. Amedisys Inc., 298 F.3d 434, 450 (5th Cir. 2002)

Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society*, *4*(1), 71-92. doi:10.1177/14614440222226271

Spitzberg, B. H., & Cupach, W. R. (2007). The state of the art of stalking: Taking stock of the emerging literature. *Journal of Aggression and Violent Behavior*, *12*(1), 64-86. doi:10.1016/j.avb.2006.05.001

Stalking Resource Center. (2012). *Stalking fact sheet*. National Center for Victims of Crime.

Standing Senate Committee on Human Rights. (2012). *Cyberbullying hurts: Respect for rights in the digital age*. Parliament of Canada. Online: http://www.parl.gc.ca/Content/SEN/Committee/411/ridr/rep/rep09dec12-e.pdf

Stoleru, M., & Costescu, E. (2014). (Re)producing violence against women in online spaces. *Philobiblon, 19*(1), 95-114. Retrieved from http://search.proquest.com/docview/1537983876?accountid=14667

Strawhun, J., M.A., Adams, N., B.A., & Huss, M. T., PhD. (2013). The assessment of cyberstalking: An expanded examination including social networking, attachment, jealousy, and anger in relation to violence and abuse. *Violence and Victims, 28*(4), 715-30. Retrieved from

http://search.proquest.com/docview/1426080449?accountid=14667

Stuart, K. (2014, December 3). Zoe Quinn: 'All Gamergate has done is ruin people's lives'. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2014/dec/03/zoe-quinn-gamergate-interview

Sweeny, M. (2014, November 12). What the law can (and can't) do about online harassment. *The Atlantic*. Retrieved from http://www.theatlantic.com/technology/archive/2014/11/what-the-law-can-and-cant-do-about-online-harassment/382638/

Tungate, Allison (2014). Bare necessities: the argument for a 'revenge porn' exception in Section 230 immunity, Information & Communications Technology Law, 23:2, 172-188, DOI: 10.1080/13600834.2014.916936.

United States Education Amendments of 1972 (Pub. L. 92‐318, 86 Stat. 235) (1972)

United States v. Alkhabaz, 104 F.3d 1492 (U.S. App. 1353, 1997)

Valenti, J. (2007, April 5). How the web became a sexists' paradise. *The Guardian*. Retrieved from http://www.theguardian.com/world/2007/apr/06/gender.blogging

Valenti, J. (2015, July 15). Why is it still legal to take creepshots of women in public places? *The Guardian*. Retrieved from http://www.theguardian.com/commentisfree/2015/nov/02/why-is-it-still-legal-to-take-creepshots-of-women-in-public-places

Walz, C. N., & Rogers III, R. L. (2014). Sixth Circuit's decision in Jones v. Dirty World Entertainment Recordings LLC repairs damage to Communications Decency actjourno-drones: A flight over the legal landscape. *Communication Lawyers*, *30*(4).

Retrieved from http://www.americanbar.org/publications/communications_lawyer/2014/september14/decency.html

Wash. Rev. Code Ann. § 9.61.260. (2004).

West, Robin L., The Difference in Women's Hedonic Lives: A Phenomenological Critique of Feminist Legal Theory (May 25, 2011). Wisconsin Women's Law Journal, Vol. 15, 2000; Georgetown Public Law Research Paper No. 11-53. Available at SSRN: http://ssrn.com/abstract=1847983

Wexler, C. (2014). *The role of local law enforcement agencies in preventing and investigating cybercrime*. Retrieved from Police Executive Research Forum website: http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf

Wingfield, N. (2014, October 14). Feminist critics of video games facing threats in 'GamerGate' campaign.". *The New York Times*. Retrieved from http://www.nytimes.com/2014/10/16/technology/gamergate-women-video-game-threats-anita-sarkeesian.html?_r=0

Working to Halt Online Abuse. (2011). Cyberstalking Statistics. Retrieved from http://www.haltabuse.org/resources/stats/2011Statistics.pdf

Working to Halt Online Abuse. (2012). *Comparison statistics 2000-2012*. Retrieved from http://www.haltabuse.org/resources/stats/Cumulative2000-2012.pdf

Ybarra, M. L., & Mitchell, K. J. (2004). Online aggressor/targets, aggressors, and targets: A

comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry, 45*(7), 1308-1316. Retrieved from http://search.proquest.com/docview/237010588?accountid=14667

Ybarra, M. L., Mitchell, K. J., Wolak, J., & Finkelhor, D. (2007). Examining characteristics and associated distress related to internet harassment: Findings from the second youth internet safety survey. *Journal of the American Academy of Pediatrics, 118(4),* el 169-1177. Retrieved from http://pediatrics.aappublications.org/content/pediatrics/118/4/e1169.full.pdf

Zharkovsky, D. (2010). "If man will strike, strike through the mask": Striking through section 230 defenses using the tort of intentional infliction of emotional distress. *Columbia Journal of Law and Social Problems, 44*(2), 193-233. Retrieved from http://search.proquest.com/docview/887915162?accountid=14667