Chapter 32
The Internet Never Forgets: Image-Based Sexual Abuse and the Workplace

Melody Lee Rood
University of North Carolina at Greensboro, USA

John Schriner
https://orcid.org/0000-0001-5588-2432
City University of New York, USA

ABSTRACT

Image-based sexual abuse (IBSA), commonly known as revenge pornography, is a type of cyberharassment that often results in detrimental effects to an individual's career and livelihood. Although there exists valuable research concerning cyberharassment in the workplace generally, there is little written about specifically IBSA and the workplace. This chapter examines current academic research on IBSA, the issues with defining this type of abuse, victim blaming, workplace policy, and challenges to victim-survivors' redress. The authors explore monetary motivation for websites that host revenge pornography and unpack how the dark web presents new challenges to seeking justice. Additionally, this chapter presents recommendations from the literature focusing on shifting cultural attitudes, effective legislation, and increased education and training.

DOI: 10.4018/978-1-6684-5598-2.ch032

INTRODUCTION

It is estimated that 1.2 trillion photos were taken in 2017; out of those images, 85% were from smartphones (Richter, 2017). In a 2015 survey that looked into "commonly regretted types of social media posts" among adults ages 18 and older in the United States, 14% shared pictures that could potentially impact their reputation at work; 10% sent intimate, sexual messages with a fear that their privacy could be breached (YouGov, 2015). While documentation culture becomes increasingly normalized with popular social media platforms like Instagram, Tik Tok, Twitter, and YouTube, a growing concern is how online presence can impact educational and/or professional prospects. It is commonplace to see social media accounts include prefacing statements in the account's bio section, declaring thoughts and opinions as one's own and not a reflection of the views of any institution in which that user is associated. Not only should people be cautious of their individual contributions to their online identities, but there is also the fear of what others can say or do without consent. Cyberbullying only exasperates this concern.

In a survey titled, "Online Hate and Harassment: The American Experience," 53% of internet users in the U.S. claimed to have experienced some form of harassment; 37% experienced severe harassment from sexual harassment to physical threats and stalking (ADL, 2019). Image-based sexual abuse (IBSA) or what's commonly known as "revenge pornography" is a type of non-consensual cyberharassment with effects that jeopardize reputation, job security, professional and educational aspirations, mental health, and in some cases, physical safety.

Revenge pornography can be defined as: "Sexually explicit images or videos of an individual, published online without their consent and with the intent to cause them distress" (Chandler & Munday, 2019). Revenge pornography is a type of cyberharassment that often directly impacts the workplace and one's job prospects. Once an image is uploaded to web platforms, it seems an insurmountable challenge to get it removed. The area of revenge pornography is akin to *doxxing*, that is, having one's personal information leaked to websites or forums—also deeply unsettling.

There is much written about cyberharassment and the workplace, although there is currently little to no academic research about specifically IBSA and the workplace. One's profession is very often the first target of abusers, as the authors explore in depth below. A major issue in dealing with IBSA is that private images can be uploaded by a single individual, but it is often shared so many times anonymously that it is difficult to find all the perpetrators. This type of mob mentality, or cyber mob, is typified by a phenomenon called *online disinhibition*. Online disinhibition, or more broadly *deindividuation* as social psychologists term it, is found when an individual experiences loss of self-awareness in a crowd: online disinhibition may be attributable to anonymity in a forum or a collective identity (Barlett & Helmstetter, 2018; Citron, 2016; Suler, 2004). Not all online disinhibition is harmful. The lack of being identified, as well as being physically separated, can help individuals with anxiety open up to strangers in online communities. That type of deindividuation is benign and can be described as the ease of communication online versus in-person, whereas *toxic deindividuation* is the ease of hurting others due to a perceived anonymity (Barlett & Helmstetter, 2018).

Toxic deindividuation can lead to less concern about social norms, and generally, the well-being of others. When individual accountability is not a concern, people may act differently than when they are identified. "It is these factors that desensitize people such that their social learning is altered to increase their willingness to engage in cyberbullying. Just as alcohol may disinhibit some people and consequently give them the courage (or stupidity) to pick a fight with a member of a biker gang at a bar, anonymity's

disinhibition and deindividuation mechanisms foster acts of online deviance in which people would not normally engage" (Lowry, Zhang, Wang, & Siponen, 2016, p. 970).

Centered throughout on concerns for the workplace, this chapter discusses how IBSA affects job prospects, security, and general wellbeing. With very little written in the academic literature about specifically IBSA and the workplace, the authors examine the literature to connect various issues such as internet abuse, deviance, online disinhibition, and technological precursors to IBSA. The authors build atop Danielle Keats Citron's exploration of cyberharassment in *Hate Crimes in Cyberspace*: "workplace sexual harassment and domestic violence were once viewed as intractable, normal features of everyday life, much as cyberharassment is viewed today" (2016, p. 22). The chapter ties together research across disciplines to encompass an up-to-date understanding of cyberharassment in the form of IBSA and challenges to the workplace and beyond.

This chapter takes a deep dive into IBSA and concerns for the future with recent research in this area including related systematic reviews (Madigan, Ly, Rash, Van Ouytsel, & Temple, 2018; Walker & Sleath, 2017), the challenge of defining terms (Maddocks, 2018; McGlynn, Rackley, & Houghton, 2017), international case studies (Chisala-Tempelhoff & Kirya, 2016; Vitis, 2019), qualitative and quantitative studies (Bates, 2017; Jane, 2018; Maddocks, 2018; Starr & Lavis, 2018), and pertinent law reviews (Citron, 2009; 2016).

BACKGROUND

Academic Research

Ophoff, Machaka, and Stander (2015) explored the impact of cyberharassment and cyber incivility, a term used specifically for aggression via email in the workplace. Cyberbullying has a negative impact on the victim-survivor's socio-emotional wellbeing. They may also experience anger, embarrassment, sadness, shame, loss of self-esteem, depression, and feelings of hopelessness (Ophoff et al., 2015).

Both qualitative and quantitative research in the area of sexting and the sharing of non-consensual personal images give us a better understanding of the scope of the problem. As thoroughly examined in Walker and Sleath (2017), quantitative research in the form of cross-sectional questionnaires provided information about sexting behavior and prevalence (both victimization and perpetration), and correlation between gender and certain sexting behaviors. Madigan and colleagues (2018) in their systematic review and meta-analysis of the literature dealing with sexting, found that multiple forms of sexting behavior are growing in prevalence, especially in older youths. Indeed, their study also found that approximately 1 in 8 youth self-report either forwarding or having a sext forwarded (Madigan et al., 2018). Qualitative research in the form of interviews provided personal accounts and further testament to the gendered nature of non-consensual image-sharing and victim blaming, particularly towards women. Walker and Sleath (2017) explored the current literature and found that in all 33 of the empirical papers identified as concerning IBSA, none of the papers examined motivation.

Much of the research in this area at the turn of the 20th century onward dealt with workplace *internet abuse*, a general term still found in the literature that encompasses internet addiction, cyberslacking, and several deviant behaviors that affect the workplace (Blažič & Gorenc, 2017; Griffiths, 2003; Vitak, Crouse, & LaRose, 2011). Typical of other literature in this area, the focus tends to be on company liability and employee productivity. Although IBSA and the workplace is not specifically examined in this research,

IBSA is clearly a type of criminal internet abuse that could also potentially have "severe implications for employers" (Griffiths, 2003, p. 90). Griffiths (2003) identified areas that employers should be aware of: online pornography use by employees and sexually-related internet crime by employees including online sexual harassment and cyberstalking.

Johnson and Chalmers (2007) analyzed employee internet traffic logs to broaden prior understanding of internet abuse that relied on self-reported surveys. The logs showed captured employee internet traffic in every *likely inappropriate* category including hate speech, pornography, gruesome content, and violence. Their findings suggested that firewall policies that block offending websites were insufficient.

Young and Case (2004) examined risk management practices in light of an epidemic of internet addiction, a new clinical disorder in the literature at the time. Young and Case (2004) surveyed companies of varying sizes and found that half of the respondents had internet use policies in place. The findings also suggested that rehabilitation of the employee was desirable to having their employment terminated in the case of treatable internet addiction. Young (2010) expanded on the older framework that relied solely on internet use policies. The internet use policy is a written agreement that is proactively coupled with employee training. This new framework also emphasized policy enforcement and rehabilitation.

The studies above show how researchers viewed the growing use of the internet in the workplace markedly different than researchers do today. While an administrative response to internet addiction of removing the employee from networked computers may have worked in the past, this tactic is seemingly ineffective in today's workplace. As cyberharassment continues to be a growing concern, these findings could be seen as crucial to laying the groundwork and orientation for a thorough exploration of IBSA in the workplace.

A Precise Vocabulary

Research in this area spans many disciplines: law, criminology, gender and women's studies, ethics, communication and media, psychology and others. Maddocks noted that "naming a new social harm presents many challenges" (2018, p. 345). By 2016, the term 'revenge pornography' had been added to Merriam Webster and Oxford English Dictionaries (Maddocks, 2018) and became the common term used in both academia and in lay articles about this social ill.

The term "revenge porn" is misleading in two respects. First, perpetrators are not always being motivated by vengeance. Many act out of a desire for profit, notoriety, or entertainment, including hackers, purveyors of hidden or "upskirt" camera recordings, and people who distribute stolen cellphone photos. The term "revenge porn" is also misleading in that it implies that taking a picture of oneself naked or engaged in a sexual act (or allowing someone else to take such a picture) is pornographic. But creating explicit images in the expectation within the context of a private, intimate relationship – an increasingly common practice– is not equivalent to creating pornography. The act of disclosing a private, sexually explicit image to someone other than the intended audience, however, can accurately be described as pornographic, as it transforms a private image into public sexual entertainment. (Franks, 2016, p. 2)

It is difficult to have a precise vocabulary when speaking about these abuses. If a researcher sets out with too broad a term, nuance or precision in the offense could be overlooked; if too narrow a term, offenses are excluded. The term 'revenge pornography' is reductive and minimizes "severe harms to a simple 'scorned ex-boyfriend' narrative" (Maddocks, 2018, p. 347). Maddocks explored alternative

terminology such as *non-consensual pornography* (NCP), *image-based sexual abuse* (IBSA), *technology facilitated sexual violence* (TBSV), and *non-consensual dissemination of intimate information*. Each term has advantages, but they also clearly come up short in fully encapsulating the severity of abuse and satisfying all instances. Through interviews, though with an overrepresentation of lawyers and legal scholars, Maddocks (2018) found that *non-consensual pornography* was the most popular term. The term foregrounds consent and "opens up connections between NCP and other non-consensual acts, positioning it as a product of a culture that undermines women's sexual consent" (Maddocks, 2018, p. 349). NCP as a term has the advantage of situating the abuse as a privacy violation and a threat to individual liberty, and it is in part because of this term and work by Mary Anne Franks and Danielle Keats Citron in the legal realm that substantial NCP laws have been passed in the United States (Maddocks, 2018). Internationally, however, the experts interviewed found issue with the word *pornography* in non-consensual pornography as the media were not created for public consumption (Maddocks, 2018). The second most popular term among those interviewed by Maddocks was the term *image-based sexual abuse*, which has garnered adoption in much of the literature in this area. This term draws attention to the "mental and physical pain caused to victims" (Maddocks, 2018, p. 350) and it is a term that builds on Liz Kelly's *continuum of sexual violence* (Kelly, 1988). This continuum is further explored below as academia begins to agree on a term. The difference in the two terms is in emphasis: "NCP refers to the product (pornography), while IBSA describes the conduct and its impact on victims (abuse)" (Maddocks, 2018, p. 350). *Technology facilitated sexual violence* (TBSV) is the first term to center explicitly on technology, recalling the rapid dissemination of media now possible, and the substantive linking as a type of sexual violence. Similar to how Computer Mediated Communication (CMC) has aided framing in communication studies, perhaps this type of sexual violence could be better understood through a technological lens. Lastly, *non-consensual dissemination of intimate information* seems to encapsulate the social problem generally enough to be used in many different scenarios while still emphasizing consent.

McGlynn, Rackley, and Houghton (2017) worked to find a suitable replacement for the popular and problematic term "revenge porn" that would emphasize sexual violence and the harm done to women. Drawing again on the groundbreaking work of Liz Kelly (1988) in conceptualizing the continuum of sexual violence, McGlynn and colleagues (2017) made the case for placing IBSA on a continuum alongside other abuses with similar characteristics. These characteristics, namely "abuse, intimidation, coercion, intrusion, threat and force" are used to control (predominantly) women (Kelly, 1988, p. 76 as cited in McGlynn et al., 2017, p. 27). Kelley noted that the continuum concept is "open to development, recognizing the necessity of intersectional analysis" (Kelly, 1988, as cited in McGlynn et al., 2017, p. 27). As abuses tend to blur into others and overlap, a continuum concept helps to plot these abuses in the understanding that each has very real effects on the victim-survivor. The problematically-named abuse "upskirting" and other abuses like sexualized photoshopping or deepfakes can all be placed on this continuum. These terms have "the effect of minimising the harms" (McGlynn et al., 2017, p. 39). The strength of the continuum concept is that victim-survivors can use the tool to better understand their experience and the "nature and extent of abuse" (McGlynn et al., 2017, p. 30). Furthermore, the concept of the continuum helps with the problem of terminology while also deepening our understanding:

The idea of the continuum based around a 'basic common character' enables connections to be revealed between different forms of abuse with important discursive, policy and legal implications. In this way, we can move beyond the discrete categories of both law and public discourse, such as 'revenge porn' or

'upskirting', to recognise the 'commonality and connections' between different forms of abuse. (Vera-Gray 2017, pp. 20–21 as cited in McGlynn et al., 2017, p. 27)

Placing IBSA on the continuum of sexual violence "enables us to see the interconnecting nature of many experiences" (McGlynn et al., 2017, p. 36). When particular laws or statutes cannot address these abuses, conceptualizing this continuum can enable "a more holistic legal and policy response" (McGlynn et al., 2017, p. 36). Workplace policy can be strategically developed to identify abuses such as IBSA and sustain a culture where this type of abuse is not permissible, even as government legislatures fail to respond appropriately. McGlynn and colleagues (2017, p. 36) emphasized that although there is definitely a breach of privacy in abuses like IBSA, conceptualizing the harms in regard to solely privacy "inhibits recognition of the gendered, sexualized and abusive nature of the practices of image-based sexual abuse."

Of the many academic areas in which IBSA may fall, criminology, and especially feminist criminology, has been used as a lens to provide substantial current research. Powell and Henry (2017) thoroughly examined the role of technology in IBSA. Powell and Henry (2017, p. 24) asserted that sexual violence is *technosocial*, that is, it "replicate[s] sex, gender and power relations that pre-exist digital technologies, while also reproducing sexual violences in both familiar and unfamiliar ways." As to terminology, Powell and Henry preferred the term IBSA as it is sufficiently broad:

Instead of focusing exclusively on the distribution of intimate images (which the 'revenge pornography' terminology implies), we focus on three interrelated behaviours that often, but not exclusively, involve digital technologies: first, the creation of nude or sexual images without consent; second, the distribution or sharing of nude or sexual images without consent (including images that were self-created by the victim or consensually created with another person); and third, the threat of distribution of nude or sexual images. (Powell & Henry, 2017, p. 120)

Powell and Henry (2017) formulated a typology that sought to provide a clear analysis of motivation: insight into the impact on victims; an accurate picture of the breadth of the problem; methods of prevention, intervention, and redress. Their five categories are: relationship retribution, sextortion, sexual voyeurism, sexploitation, and sexual assault. The typology functions as both a classification and an orientation with which to examine abuse in empirical studies.

Victim Blaming

Victim blaming is the act of shifting the perspective or narrative of a situation to insinuate or clearly declare that a crime was committed due to the actions or behaviors of the victim-survivor. "Therefore, victim blame often flows from this assumption that the victim was responsible for the crime being acted upon them. For example, a victim of revenge porn may be viewed as responsible for taking and sending an image to someone in the first place" (Starr & Lavis, 2018, p. 428). Many victim-survivors of IBSA who chose to seek justice are often bombarded with additional cyberharassment in the form of victim blaming. Langlois & Slane (2017, p. 122) noted that the "two key pieces of information for a 'successful' revenge pornography campaign [are] intimate pictures and the identity of the victim." These researchers examined revenge pornography using Actor-Network Theory, that is, how human and non-human actants are "involved in, associated with, and give shape to revenge porn and connect it to different information networks" (Langlois & Slane, 2017, p. 122). With these two pieces of information, the OP (original

poster) is establishing that the victim is the target. "Naming the victim also increases the likelihood that other people in the victim's offline life (e.g. current partner, family members, boss) will be exposed to these intimate images" (Langlois & Slane, 2017, p. 124).

While image-based sexual abuse can happen to anybody, the victim-survivors are generally women. According to the Cyber Civil Rights Initiative, 90% of revenge pornography victims are women, thus it cannot be ignored that this type of harassment is a gendered issue as well as a form of abuse included in rape culture as a whole (Hall & Hearn, 2018; Franks, 2016). Only recently have researchers explored the gendered nature of IBSA and the motivation via perpetrators' accounts. Hall & Hearn (2019) through discourse analysis continued their work by building on Schwalbe's (2014) research in exploring practices of men and *manhood acts*. Their findings note that "power, control and (hetero)sexuality were the main underlying themes throughout our analysis. What linked all the posts we encountered was victim blaming" (Hall & Hearn, 2019, p. 162). Posting sexually explicit images were "compensatory manhood acts" and elicited a perception of regaining control (Hall & Hearn, 2019, p.162). Victim blaming and reputation destruction is also rampant on social media: "Social media now, is like the town square in the dark ages. We haven't yet figured out our laws to govern the way we treat each other. Back then, if suspected women weren't burnt and boiled to death, their reputation was. Revenge porn now is the public shaming of women, onlookers are the townspeople and some throw stones" (Wilson, 2015).

Victim blaming is a familiar issue within the women's rights movement. Pervasive comments that victim-survivors need to toughen up or that they somehow invited the abuse are not uncommon. These views help solidify and normalize a culture of abuse. Citron (2016) articulated that workplace sexual harassment used to be normalized in similar ways up until recently. The same can be said for domestic violence. Victim-survivors were dismissed as being too sensitive, inviting the sexual harassment, or the abuse was not serious enough because they did not immediately leave abusive partners. Citron (2016) stated that social attitudes need to change for survivors to be taken seriously. "During the 1960s and 1970s, the women's movement had to change how society saw and responded to domestic violence and workplace sexual harassment. That struggle provides important insights for an agenda to combat cyberharassment" (Citron, 2016, p. 91).

Workplace Policy

In the Walker and Sleath (2017) review above, there was a scarcity of research aimed at guiding appropriate administrators about IBSA in the workplace. Academic research is rich with literature focusing on workplace policy for combating cyberharassment in general. Outside of academic research, organizations increasingly offer guidance for workplace policy in confronting IBSA.

Piotrowski (2012) found that administrators and organizational leaders may not be aware of the severity of cyberharassment in the workplace. The researcher placed cyberharassment in the context of workplace bullying and conducted an analysis of over a decade of literature in this area. To limit sexual harassment lawsuits that were based on, for example, inappropriate emails, Piotrowski (2012) suggested that management periodically strengthen their company harassment policy. Any form of "e-harassment" should be viewed "through the lens of a) threat assessment, b) crisis management, and c) employee safety" (Piotrowski, 2012, p. 49). An organization development model should be established with the following coping strategies: zero tolerance standards for cyberbullying; professional counseling for interpersonal conflicts that arise in the workplace; anger management counseling; unambiguous policy in handling complaints; manager vigilance for warning signs of "targeted" employees; confidentiality

and mediation; preserving the rights of workers and being aware of legal liability; maintaining a safe and positive work environment; and threat assessment that focuses on new technologies that can be avenues for cyberabuse (Piotrowski, 2012). These recommendations work well as they can adapt to both changes in technology and in social mores.

Langlois and Slane (2017) conducted an analysis of the revenge pornography site *myex.com* and collected a sample of posts and comments. While the site often displayed the victim's name and location, some comments contained veritable threats (e.g., "Do you have her work info? I want to show her naked to her boss") (Langlois & Slane, 2017, p. 125).

As intimated earlier, a useful definition of workplace harassment is "repeated and persistent attempts by one person to torment, wear down, frustrate or get a reaction from another" (Brodsky, 1976, as cited in Paul, 2015, p. 1). Workplace cyberharassment as a newer "networked" type of harassment has the potential to be exacerbated: it's important to be reminded that "consistent networked contact makes threats more palpable and harder to mitigate" (Vitis, 2019, para. 33).

Arnold (2014) described how revenge pornography is a "vicious new way to smear someone's professional reputation." Arnold's (2014) suggestions for mitigating revenge pornography in the workplace centered around supporting the victim-survivor. It is suggested that the employer speaks with the employee about the incident as soon as possible, provided the employee wishes to speak: if not, it is suggested to let the employee know that the organization is committed to a safe work environment (Arnold, 2014). Furthermore, the employer should: provide materials from support organizations such as *Without My Consent*, *End Revenge Porn*, and *Women Against Revenge Porn*; limit the situation in the workplace; work with the IT department to block offensive materials from workstations (Arnold, 2014). Arnold (2014) echoed Piotrowski (2012) above in updating policy: "employers should strongly consider implementing policies designed to minimize the effect of revenge porn in the workplace and on the individual" as well as "give serious thought to understanding the emotional devastation revenge porn victims experience, and take steps to minimize the harm to victims and your own company."

To conclude this section on workplace policy, the work of Jane (2018) examined the very real economic damage caused by IBSA, gendered cyberhate, and cyberharassment in general: "once reputationally damaging material is circulated about them online, it is all but impossible to remove and has a potentially unlimited lifespan, thereby potentially sabotaging their work prospects indefinitely" (Jane, 2018, p. 586). Especially in precarious labor contexts where so much work is done online, economic vandalism affects livelihood as well as personal wellbeing: hard-fought protections for "women from sexual harassment in the Fordist workplace provide little to no protection to women in new economy sectors such as game design" (Elliot, 2015 as cited by Jane, 2018, p. 587).

CHALLENGES

Civil Rights Issue

The Civil Rights Division of the U.S. Department of Justice is responsible for enforcing Federal statutes that prohibit discrimination based on race, color, national origin, sex, disability, and religion. These Federal laws prohibit discrimination in education, employment, credit, housing, public accommodations, voting, and in certain federally funded and conducted programs, among other areas. In addition, the Division prosecutes actions under several criminal civil rights statutes that are designed to preserve

personal liberties and safety. The Division can also seek relief for persons confined in public institutions where existing conditions deprive residents of their constitutional rights. (Civil rights, 2014)

Cyberspace is often viewed as separate from reality, making it difficult to make the connection to civil rights issues. However, what happens on the internet can have real consequences that directly impact personal liberties to pursue education and employment. This is highlighted even further by the fact that the majority of IBSA victim-survivors are women who must take extreme measures to undo the damage of this particular type of cyber assault. Actions like legally changing your name and erasing your online identity are just a small portion of the added labor to lead a normal life again. "The costs of regaining control over one's online self are enormous. They range from submitting constant 'takedown' requests to enduring cyberstalking, rape threats, and offline harassment. This leads many victims to enter 'internet exile' undermining their basic human rights to freedom of expression on and offline" (Maddocks, 2018, p. 17). When opportunities are being hindered due to IBSA and victim blaming, those women are barred from pursuing employment or an education, among other possibilities.

No one should be expected to withdraw from online activities to avoid targeted attacks… One cannot abandon online platforms without great cost, just as sexually harassed workers and abused wives could not leave the workplace and home without a steep price. Networked tools are indispensable to every aspect of our lives: jobs, professional opportunities, socializing, civic engagement, and self-expression. Victims cannot just 'get rid of the technology' to prevent the abuse. (Citron, 2016, p. 101)

Representative Cases

In several cases of general online abuse, victim-survivors have had their personal and professional lives put in jeopardy. In one scenario, a blogger under the pseudonym, Anna Mayer, had anonymous users post false accusations about her being fired from previous jobs for "sexual misconduct" (Citron, 2016, p. 2). The poster also included the name of Mayer's then supervisor. "Many posts were explicitly designed to make her unemployable… 75 percent of the links appearing on the first page of a search of her name were the attack sites and disparaging posts. Given how unusual her real name is, Mayer ultimately decided to include a disclaimer on her resume, warning employers about what they would inevitably find if they searched her name online" (Citron, 2016, p. 3).

In an example of IBSA cited by Citron, one woman named Holly Jacobs, was tipped off that private, sensitive images that she had sent to an ex-boyfriend were posted on a revenge pornography website. Later she discovered that her sexually explicit photos were on several sites, some that included her full name, address, and place of employment. Some of the sites claimed that she was unemployed, therefore attempting to make money through sexual interactions, leading to a flood of disturbing messages from strangers. Somebody created a fake social media account for her on Facebook, but when she requested the account be removed, Facebook demanded that she prove her identity. Concerned that one of the several harassers involved could intercept her proof of personal identification, Jacobs did not comply, and it was not until the account creator posted her nude photograph that the fake account was taken down. When Jacobs tried to have her images removed from various websites by invoking her copyright to the images, she was often left with no response or a request for a removal fee. What started as possibly one individual posting to a revenge pornography site ended with numerous cyber harassers targeting Jacobs' livelihood. "The Human Resources Department at her university received an anonymous phone call

that accused her of 'masturbating for her students and putting it online.' Because she taught students as part of her doctoral program, the accusations could interfere with her degree" (Citron, 2016, p. 46). At one point, Jacobs received an anonymous call demanding that she meet with the stranger by a specific time or else he'd send her intimate images to her place of employment. For fear of being unemployable, Jacobs legally changed her name (Citron, 2016).

In both the Mayer and Jacobs cases, their work life was threatened by online abuse. By including Mayer's then supervisor in one of the false posts, her workplace became involved. Mayer made the decision to explain the situation to her supervisor, which Citron described as a "painful and embarrassing task" (Citron, 2016, p. 2). Even though the supervisor was supportive, her anxiety about future employment was not put to rest. In the case of Jacobs, her colleagues were sent nude photographs because she did not respond to the anonymous caller. "Although the firm assured her that no one would pay attention to the e-mails, she could not help but worry about their impact. She received frightening e-mails at work and feared that she would be physically stalked when going home" (Citron, 2016, p. 46). It is also worth considering how changes in perception from professional colleagues after becoming a victim-survivor to IBSA can potentially shift the workplace environment, an area that requires further research.

International Case Studies

Much of the empirical research on IBSA has been conducted in Australia, the United Kingdom, and the United States with only "limited research [that] has been cited across Asia" (Vitis, 2019, para. 2). This has led to a hegemonic understanding that "Northern victims/survivors set the scholarly agenda for 'all' women" (Mohanty, 1988 as paraphrased by Vitis, 2019, para. 2). As discussed throughout this chapter, legislation exists in many jurisdictions across the world to combat IBSA, but from the research, still "currently little is known about the prevalence, causes and impacts of this problem globally" (Powell & Henry, 2017, p. 118).

In a case study on IBSA in Singapore, Vitis (2019) viewed the abuse using tools and lenses described above. Vitis built upon Kelly's (1988) continuum of sexual violence as well as noting the placement of IBSA on the continuum in McGlynn and colleagues' study (2017). Vitis then employed Powell and Henry's (2017) work on typologically categorizing abuses, namely: sextortion, sexploitation, and sexual voyeurism as the most common in this study.

Vitis's (2019) study consisted of data collected from a sexual violence service provider in Singapore from January 2016 to December 2016. Of 338 total cases, "60 (18%) involved the use of technology to either facilitate or record violence" (Vitis, 2019, para. 21). Of these 60, there were 30 cases of IBSA. The most common form of abuse in this study was sextortion, "where images were coerced *from* women and used as a tool *of* coercion and blackmail" (Vitis, 2019, para. 22). Following sextortion, the other types were non-consensual distribution of intimate images (NDII), and sexual voyeurism. Vitis (2019) explored the work environment of domestic workers and how in-home surveillance is increasingly prevalent: "while digital technologies have become normalized techniques of governing employee performance (Ball, 2010, p. 87), for domestic workers video surveillance intrudes private spaces where labour and living intertwine" (para. 29). The fourteen sextortion cases in Vitis highlighted how "digital technologies permeate domestic violence because of their propensity to facilitate coercive control with greater ease, intensity, and immediacy" (Vitis, 2019, para. 31).

Chisala-Tempelhoff and Kirya (2016) explored IBSA in Malawi and Uganda. Through case studies and examinations of current laws, the authors believed that specific legislation, rather than relying

on ineffectual existing laws, is the way forward in these countries. IBSA is a type of "cyber violence" against women and a scourge that "demands a swift and specific response" (Chisala-Tempelhoff & Kirya, 2016, p. 2). As in other areas of the world, "harmful digital behaviours, such as revenge porn, are often framed as a problem of user naiveté rather than GBV (gender-based violence)" (Chisala-Tempelhoff & Kirya, 2016, p. 2).

Websites and Section 230 of the Communications Decency Act (1996)

The *clearnet*, or the normal open web found through an internet browser, has been the home to sites that host revenge pornography. Revenge pornography websites often use the Communications Decency Act, Section 230, as a defense for their existence: as the content is user-submitted, the sites avoid accountability by claiming to be a channel, whereas third parties are the content-creators. These sites earn money through advertising, directing users to pornography sites, and sometimes a content-removal fee. Famous examples like myex.com were reported to have charged victims upwards of $400 to remove the damaging content (Hall & Hearn, 2018). In 2018, a federal court ordered the site to be shut down. Other sites have also been issued shut down orders and were not entitled to immunity based on the Communications Decency Act (Minc, 2017). Hunter Moore's website *IsAnyoneUp?* (and subsequent similar sites like *You Got Posted* and *Pink Meth*) have been the subject of lawsuits in U.S. Federal Court (ViaView, Inc. v. Blue Mist Media, 2012; Talley v. Chanson, 2014): "Several victims have filed lawsuits based on the loss of educational and employment opportunities from the online posting of their naked photos" (Burris, 2014, p. 2237). Kevin Bollaert, who was the owner of *ugotposted.com* revenge pornography site, was sentenced to 18 years in prison (Cox, 2015). Accountability of site operators tends to stem from crimes of extortion, hacking, and identity theft, rather than specifically hosting and soliciting IBSA material. However, even as these sites continue to be removed either through legal battle or being removed by their host, more websites pop up. In addition, the damage done is often irreversible as images have already moved to other corners of the clearnet, and eventually to the dark web, making victim-survivor redress much more difficult. Once the images are used to anonymously crowdsource harassment with the attempt to ruin a person's life, often the first line of attack is targeting the victim's career.

The aforementioned *IsAnyoneUp?* made contributing revenge pornography images into a "well-oiled process, with submitting users supplying Moore with pictures as well as the portrayed victim's 'full name, profession, social-media profile and city of residence'" (Morris, 2012, as cited in Stroud, 2014, p. 170). The site was live for over a year and Moore reported that "as of November 2012, he received around 35,000 submissions each week" (Hill, 2012, as cited in Stroud, 2014). Moore believed that the content was "around about 50% revenge pornography and 50% 'self-submitted' pictures" (Hill, 2012, as cited in Stroud, 2014, p. 170). The re-launched version of the site, also now offline, boasted "I am making something very scary but yet fun" and it will be launched "with all the IAU (*IsAnyoneUp?*) content and all new content" ("Hunter Moore," 2013). This clearly shows that even when sites are taken down, their content has been shared and saved for a service rebranding or reboot. The revenge pornography site *Pink Meth* worked in much the same way, with an emphasis on connecting the image content to the victim's personal social media. This site moved to the dark web where legal pressure and content takedowns were potentially a thing of the past.

From the Clearnet to the Dark Web

It is very difficult for the victim-survivor to successfully petition a site to take down personal intimate images, and the problem is exacerbated with technology that obscures server or service location. The dark web is composed of websites whose web servers cannot be forced to remove content because their location and service host are hidden from both law enforcement and from site visitors. Anonymity networks such as Tor, i2p, and Freenet are three popular technologies that potentially provide anonymity to the website and the visitors of the website. Whereas victim-survivors can try to redress their rights with the hosting website or the service host of the website itself, most victim-survivors meet roadblocks or law enforcement that fail to recognize the severity of the problem (Citron, 2016). Whereas the European Union continues to develop its *Right to be Forgotten*, or *Right to Erasure* in its highest courts, much of the world lacks real legislation or processes to protect victims of cyberharassment and IBSA from continuing to see their unauthorized content listed in search engines and across the web. Thinking about sites that cannot be taken down leads to questions such as: what if there is technically no way to enforce "the right to be forgotten" and where can a victim find redress?

The dark web is accessible through specialized software that works to keep a visitor anonymous as well as keeping the website's actual location and IP hidden. The Tor Browser, when used properly, can provide a reasonable amount of anonymity. Most, if not all, of the dark web revenge pornography websites are accessible through the Tor network. Put briefly, the Tor Browser sends one's connection through three other machines ostensibly around the world to meet at a rendezvous point for the website, which has also obscured its real location. Each hop in the circuit only knows where the connection came from and where it is going, but never the full picture (i.e. never the full request or circuit). In this way, by keeping its location and service provider obscured, it cannot easily be taken down through legal battles or even sent takedown requests.

Despite some successes in revenge pornography websites being taken offline, there is still far to go in making certain that IBSA cannot find a home on the world wide web. The spinoff site *IsAnybodyDown?* was shut down by the United States Federal Trade Commission ("FTC," 2018) and the owner of the site agreed to a settlement and the requirement to permanently delete all of the material he had collected through the site's operation (Scharr, 2015).

Although some legal headway has been made with acknowledging the severity of IBSA, and the most prominent search engines will remove non-consensual images and revenge pornography from results (Beauchere, 2015; "Remove unwanted & explicit personal images from Google", n.d.), revenge pornography sites still exists on the clearnet despite not being indexed. When the legal battles become too costly or interruptive, the site operators find that "Revenge porn is more resilient on the dark web. Case in point: After one notorious dark web revenge porn site was shut down, an apparent archive of material from it lives on" (Cox, 2015). Mentioned briefly above, the revenge pornography website Pink Meth was on the clearnet before moving to the dark web. Due to a lawsuit and having their domain names suspended, the site operator opined "Projects like Pink Meth are simply much more suited as a hidden service as opposed to a regular website" (Gilbert, 2014). The dark web version of Pink Meth was eventually seized along with 27 other sites in a joint operation by Europol, the FBI, and U.S. Immigration and Customs Enforcement (Gilbert, 2014).

Monetization

Revenge pornography website owners on the clearnet have the motivation of monetization. "'Why should I care?' Mr. Moore said, taking a sip of his drink. 'It's not my life. It's literally just a business. It's stupid not to monetize it'" (Roy, 2012). Having a site of this kind on the clearnet is far more lucrative than a dark web site: search engines bring visitors and advertising revenue well surpasses site operation costs. Moore had boasted that his site had "reached $30,000 in a month" (Morris, 2012 as cited in Stroud, 2014).

The economic incentives to running a revenge pornography site are substantial. As examined in thorough detail in Langlois and Slane (2017), the material is user-generated and as long as a site operator can stay within the legal bounds of the Communications Decency Act, Section 230, they can run their site on the clearnet. Indeed, Langlois and Slane (2017, p. 127) noted that the revenge pornography site myex.com ironically stated in its Terms of Service that users "will not use the website to harass or invade the privacy of another person (including the dissemination of personal information)." The site itself not only had input fields for personal information of the victims, but its tagline was "Get the dirt before you get hurt or submit your ex gf and bf and get revenge!" (Langlois & Slane, 2017, p. 126). The Terms of Service was clearly meant as legal protection that ran entirely counter to the site's *raison d'être*. To use the site it is also required that the users "have the written consent or release of each identifiable person in the submission to use their name or likeness" but of course no proof of consent was required to post (Langlois & Slane, 2017, p. 127).

The site myex.com clearly sought to monetize IBSA and Langlois & Slane (2017) deeply explored their business model. "Here, revenge porn is less about promoting some kind of moral claims in relation to free expression and rather about building up and defending an information repository that can be monetized" (Langlois & Slane, 2017, p. 126). By shifting from brazen to strategically shielded operations, the site continued running profitably and was still entirely accessible via the clearnet during Langlois & Slane's study. The site was taken down by a federal court order at the request of the United States Federal Trade Commission and the State of Nevada in early 2018 ("FTC," 2018). The site ran for five years which shows that the monetization motivation will continue to be a challenge until appropriate laws protecting victims from website safe havens of this kind are enacted.

SOLUTIONS AND RECOMMENDATIONS

There are several layers to IBSA that make it difficult for victim-survivors to seek justice. First, there are the overarching social and cultural issues like general violence against women, non-consent fetishization, rape culture, double standards, victim blaming, and cursory preventative measures such as risk management (Maddocks, 2018; Bates, 2016). Then there is the issue of toxic online disinhibition, which makes hurting others easier due to perceived anonymity (Barlett & Helmstetter, 2018). Victims affected by toxic online disinhibition who chose to speak out can get stuck in a cycle of experiencing even more harassment from cyber mobs who often reach out to employers, affecting one's job security and livelihood. The damaging images or false information that cyber mobs share cascades to a point where finding individual perpetrators becomes impossible. From a financial standpoint, some victim-survivors must pay hundreds of dollars to have images removed from revenge pornography sites just to have the images pop up elsewhere and potentially move to the dark web. This does not even include the financial privilege it takes to combat cyberharassment from a legal standpoint. "Tort remedies for

defamation, intentional infliction of emotional distress, and privacy invasions exist only in theory for some victims due to the high cost of litigation and the absence of privacy protections" (Citron, 2016, p. 24). Those privacy concerns just highlight the issue that victims can't always turn to civil rights laws as they are currently written. In addition, law enforcement often lacks the training and knowledge to address these situations. These are just some of the issues with combating IBSA, and there is no simple solution to the problem.

Changes in Cultural Attitudes

Major changes in cultural attitudes about internet norms could be an important step to dealing with IBSA. Just as cultural attitudes changed about sexual harassment in the workplace and domestic abuse, the "Wild West" culture of the internet can shift as well (Citron, 2016, p. 79). Citron also recommended that service providers of spaces like revenge pornography websites be held accountable, not just the individuals who post on those sites: "...moving beyond a focus on harassers as the sole problem and addressing the responsibilities of a narrow class of online service providers: sites that encourage cyber stalking or nonconsensual pornography and make money from its removal *or* that principally host cyber stalking or nonconsensual pornography" (2016, p. 25). The hope is that the more these service providers are held accountable and even criminalized, cultural attitudes about their existence will shift in a negative way, preventing the creation of more revenge pornography sites.

In addition, cultural attitudes about sexting in general most likely need to shift in order to have constructive conversations about seeking justice for IBSA victim-survivors. How does the current culture reconcile the normalcy of sexting and sharing intimate images with a partner, while also recognizing the very real dangers of revenge pornography? Sexting is a predictor of sexual behavior (Madigan et al., 2018) as well as largely viewed as a healthy part of a relationship (Walker & Sleath, 2017). "Telling us not to do it is like preaching abstinence to teenagers. It's grossly unrealistic and it doesn't work. It is also beyond outdated and is just plain ignorant to how modern dating works" (Wilson, 2015). The reality of sexting frequency conflicts with the discourse around online risk management. It is easy to warn people about the possible repercussions for sending intimate messages, while failing to realize that it simply does not stop people from doing it. Perhaps the cultural attitude should not be about stricter online risk management, which only adds to a culture of victim blaming, but accepting that sexting is a current reality for many individuals, and those people deserve to have their messages kept private; violating the privacy of those who send intimate messages should be punishable, not the act of sending them in the first place.

Privacy Protection

Another recommendation is to make legal action more accessible by allowing victims to use pseudonyms as a protective measure as they seek justice. This extra form of privacy protection allows individuals to pursue legal action without the fear of a public trial affecting their employment or employment prospects. Similarly, Citron (2016) suggested that laws create protections to safeguard individuals from having online abuse held against job candidates, allowing victims a chance to explain the situation before any hiring decisions can be made. "Evidence increasingly supports the argument that employers are unlikely to ignore cyber harassment. As behavioral economists have shown, we tend to credit what we first learn about someone… Recent studies suggest that information's prominence in searches is often used as a

proxy for reliability, which is terrible news for cyber harassment victims" (Citron, 2016, p. 183). While legal reform might not change the attitudes employers have around victim-survivors of image-based cyberharassment, it will at the very least give those individuals legal protections until the cultural attitudes catch up. "The overall goal of this agenda is to protect the equality of opportunity in the information age" (Citron, 2016, p. 25).

Increased Education and Training

Education is a key component to creating effective solutions for all cyberbullying and harassment, but especially IBSA. Police often lack the training to understand cyber threats. Victim-survivors have expressed feelings of humiliation when police refuse to take their claims seriously or blame the victim for cyber assault, indicating that not only is there a technical lack of training, but also a lack of sensitivity. "Interviewees in the United States described how underage victims had been accused by police of creating child pornography when they sought help after their private images were disclosed" (Maddocks, 2018, p. 355). In some cases, police lacked the understanding of the few laws that could potentially protect victims of IBSA, such as copyright laws. If the victim took the photo, they are the creator of that image, and thus copyright protections are automatic whether registered or not. "Under federal law, copyright holders have exclusive rights to reproduce, distribute, and publicly display their copyrighted work" (Citron, 2016, p. 47). However, in one scenario, local law enforcement told the victim-survivor that since they shared an intimate photograph with a partner, it was his property to which he could do whatever he wished. "Another officer said his department lacked jurisdiction over the attacks because they occurred on the Internet" (Citron, 2016, p. 47).

Law enforcement is not the only area in which education needs to improve. Parents and schools can also play an important role in the discourse around digital citizenship, but they too need the proper training. Understanding how toxic online disinhibition perpetuates cyberharassment might give adults the tools they need to explain the pervasiveness of cyberbullying as something beyond "a few bad apples"–that is, kids could be contributing to cyberharassment without much thought, but to the detriment of those being targeted. Understandably, not all schools can afford additional training or programming, but early education should continue to be a part of the conversation to combat cyberharassment.

Finally, the workplace needs to develop education and training that adapts with changing technological realities such as IBSA and other forms of online abuse. Given that so many perpetrators begin their harassment with an attempt to get the victim-survivor fired or make that individual unemployable, a strategic plan should be created to address this issue and must be understood by all employees. Training should make it clear that any action that perpetuates or encourages the spread of IBSA will not be tolerated. For example, if employees are made aware of circulating sensitive images of a colleague, any attempt to view the items *after* receiving that information could be treated as a sexual harassment violation. In addition, it would be beneficial to invite experts to help facilitate the training to ensure that it is being taken seriously and not treated as an obligation by reluctant management.

Updated Laws

As previously stated, civil rights laws can protect individuals from harassment actuated by prejudice against identity markers like race or religion. Unfortunately, online abuse against individuals prompted by bias doesn't generally invoke the same enforcement. "Civil rights law has the same potential for

civil rights violations in cyberspace. Law could signal that online abuse produces corrosive harm to individuals, groups, and society, just as law helped appreciate the social harms of sexual harassment in the workplace" (Citron, 2016, p. 128).

Citron (2016) suggested that laws be updated to consider the changing technology that makes cyberharassment and cyber stalking possible. "Stalking and harassment laws should cover any means, methods, or technologies exploited by perpetrators to stalk and harass victims" (Citron, 2016, p. 143). In addition, Citron advocated for harsher punishments for IBSA given the severe and devastating effects it can have on an individual's mental health. In a study titled "Revenge Porn and Mental Health: A Qualitative Analysis of Mental Health Effects of Revenge Porn on Female Survivors" published in *Feminist Criminology,* qualitative interviews revealed participants who were survivors of IBSA experienced "trust issues, posttraumatic stress disorder (PTSD), anxiety, depression, suicidal thoughts, and several other mental health effects" (Bates, 2016, p. 1). The mental health consequences of revenge pornography are like those experienced by a rape survivor, as were the coping mechanisms used (Bates, 2016). Mental health deterioration is just one reality of cyberharassment, but there is the added threat of physical safety and adverse effects to one's career–all which can amplify that mental and emotional component. "Classifying cyber harassment as a felony is warranted. The harm is serious enough to justify the punishment meted out for felonies" (Citron, 2016, p. 144).

In cases of IBSA, unlawful surveillance laws can be updated to include self-captured images or images shared consensually, but with the understanding that the consent is contextual and not extended to others.

What individuals share with lovers is not equivalent to what they would share with the world. Common sense teaches us that consent is contextual; consent does not operate as an on/off switch. The nonconsensual sharing of an individual's nude photo should be no different: consent within a trusted relationship does not equal consent outside of that relationship. We should no more blame individuals for trusting loved one with intimate images than we blame someone for trusting a financial advisor, support group, or waiter not to share sensitive personal information with others. Consent's contextual nature is a staple of information privacy law. Best practices and privacy laws make clear that permitting an entity to use personal information in one context does not confer consent to use it in another without the person's explicit permission. (Citron, 2016, pp. 147-148)

Lawmakers should also seek to make the language of legislation as unambiguous as possible so they can criminalize intentional IBSA without crimes slipping through loopholes due to vague terminology. Terms like *sexually explicit*, *disclosure*, *image*, *harm*, and *contextual consent* (Citron, 2016) are just a few examples where clarification is crucial in the process of holding perpetrators accountable. Additionally, legislation should leave room for potential technological abuses that may arise in the future. Finally, states should amend civil rights laws to recognize and restrict any cyberharassment that "interferes with victims' civil rights, including employment, contracts, education, and expression" (Citron, 2016, p. 155).

FUTURE RESEARCH DIRECTIONS

As mentioned by many researchers above, the issue of IBSA and the workplace is still quite new. By keeping up to date with current research, scholars and activists alike work towards prevention and appropriate redress when it occurs.

By employing the tools provided by McGlynn and colleagues (2017), IBSA can be placed on a continuum of sexual abuse. More researchers may adopt methods from Vitis (2019) and use the typological tools from Powell and Henry (2017) on empirical studies to categorize the abuses, leading to a better understanding of the severity of the crime.

As technologies change, deepfakes will likely come to the forefront of non-consensual production and sharing. Unlike other kinds of IBSA, deepfakes do not require intimate images. By using the frameworks above, researchers are ready to expand and contextualize the abuse. Further research in areas such as communications, criminology, and gender studies will be necessary as these technologies appear.

Future research should continue studying varied communities, especially marginalized ones who are found to have barriers to support. Varied case studies would attest that "contextual variances highlight the importance of localised analyses focused on private, hidden and obscuring conditions" (Vitis, 2019, para. 42). More empirical data would be valuable in examining the severity of abuse in different sectors and work contexts as well as "formulating a taxonomy of technology-assisted or -enabled harassment in the workplace" (Jane, 2018, p. 588). Bowling and Beehr (2006) noted that much of the research examined the abuse from the viewpoint of the victim-survivor. It's necessary to further explore the perpetrator's perspective and motivation as well as further examine the gendered nature of IBSA. Researchers clearly also need to focus on awareness-raising and assisting in the "implementation of programs to help support victims of image-based abuse" (Starr & Lavis, 2018, p. 436).

CONCLUSION

This chapter framed image-based sexual abuse, commonly called revenge pornography, as a kind of cyberharassment that greatly affects the workplace, potentially one's career *in toto*, and one's wellbeing. IBSA may be best understood as an abuse that can be placed on a continuum of sexual violence. Scholars and activists do not always agree on terminology and it remains contentious due to the motivation of perpetrators and the desire to encompass both nuanced and general abuses alike. Some terminology implies a focus on what is labeled as *pornography*, while others focus on the *abuse*–moving away from language that potentially contributes to a victim blame culture. This is paramount, considering the all-too-common responses to IBSA from the general public as well as law enforcement which often places blame on the victim-survivor.

Websites on the clearnet that host or solicit revenge pornography materials are now held accountable after, in some cases, years of profits at victim-survivors' expense; monetization as a motivator will continue to be a challenge. Some of these sites have moved to the dark web and present new challenges to victim-survivor redress.

IBSA should be recognized as a civil rights issue because it specifically affects the livelihood of those impacted. This includes the right to seek and maintain employment without the fear of having non-consensually posted images used against them. Laws must be adapted and amended to include privacy protections for victim-survivors while taking full measures to bring actions against perpetrators. Changes in both culture and legislation are necessary in order to further workplace protections and support victim-survivors' safety.

REFERENCES

ADL. (2019). *Share of adult internet users in the United States who have personally experienced online harassment as of December 2018* [Graph]. Statista. Retrieved from https://www.statista.com/statistics/333942/us-internet-online-harassment-severity/

Arnold, M. (2014) *Revenge porn: A disturbing picture*. Retrieved from http://www.mondaq.com/unitedstates/x/333158/Discrimination+Disability+Sexual+Harassment/Revenge+Porn+A+Disturbing+Picture

Ball, K. (2010). Workplace surveillance: An overview. *Labor History*, *51*(1), 87–106. doi:10.1080/00236561003654776

Barlett, C., & Helmstetter, K. (2018). Longitudinal relations between early online disinhibition and anonymity perceptions on later cyberbullying perpetration: A theoretical test on youth. *Psychology of Popular Media Culture*, *7*(4), 561-571.

Bates, S. (2017). Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors. *Feminist Criminology*, *12*(1), 22–42. doi:10.1177/1557085116654565

Beauchere, J. (2015, July 22). *'Revenge porn': Putting victims back in control*. Microsoft on the Issues. Retrieved from https://blogs.microsoft.com/on-the-issues/2015/07/22/revenge-porn-putting-victims-back-in-control/

Blažič, B. J., & Gorenc, M. (2017). Deviance in the internet use in working environment: Key factors and remedies based on an exploratory study. *Review of European Studies*, *9*(4), 52. doi:10.5539/res.v9n4p52

Bowling, N., & Beehr, T. (2006). Workplace harassment from the victim's perspective: A theoretical model and meta-analysis. *The Journal of Applied Psychology*, *91*(5), 998–1012. doi:10.1037/0021-9010.91.5.998 PMID:16953764

Brodsky, C. M. (1976). *The harassed worker*. Lexington Books.

Burris, A. (2014). Hell hath no fury like a woman porned: Revenge porn and the need for a federal nonconsensual pornography statute. *Florida Law Review*, *66*, 2325.

Chandler, D., & Munday, R. (2019). Revenge porn. *Dictionary of Social Media*. Oxford University Press. Retrieved from https://www.oxfordreference.com/view/10.1093/acref/9780191803093.001.0001/acref-9780191803093-e-1231

Chisala-Tempelhoff, S., & Kirya, M. T. (2016). Gender, law and revenge porn in sub-Saharan Africa: A review of Malawi and Uganda. *Palgrave Communications*, *2*(1), 16069. Advance online publication. doi:10.1057/palcomms.2016.69

Citron, D. K. (2009). Law's expressive value in combating cyber gender harassment. *Michigan Law Review*, *108*(3), 373.

Citron, D. K. (2016). *Hate crimes in cyberspace*. Harvard University Press.

Civil rights. (2014, June 16). *United States Department of Justice*. Retrieved from https://www.justice.gov/otj/civil-rights

Cox, J. (2015). *Revenge porn returns to the dark web*. Vice. Retrieved from https://www.vice.com/en_us/article/53988z/revenge-porn-returns-to-the-dark-web

Elliot, A. (2015). Gamergate: Gender at work in the new economy [seminar]. School of Social and Political Sciences, The University of Sydney.

Franks, M. A. (2016). *Drafting an effective 'revenge porn' law: A guide for legislators. Cyber Civil Rights Initiative*. Retrieved from https://ssrn.com/abstract=2468823

FTC. (2018, June 21). *Nevada obtain order permanently shutting down revenge porn site myex*. Federal Trade Commission. https://www.ftc.gov/news-events/press-releases/2018/06/ftc-nevada-obtain-order-permanently-shutting-down-revenge-porn

Gilbert, D. (2014). *Pink meth revenge porn darknet website shut down by FBI in Operation Onymous*. International Business Times UK. Retrieved from https://www.ibtimes.co.uk/pink-meth-revenge-porn-darknet-website-shut-down-by-fbi-operation-onymous-1474013

Griffiths, M. (2003). Internet abuse in the workplace: Issues and concerns for employers and employment counselors. *Journal of Employment Counseling*, *40*(2), 87–96. doi:10.1002/j.2161-1920.2003.tb00859.x

Hall, M., & Hearn, J. (2018). *Revenge pornography: Gender, sexuality and motivations*. Routledge, Taylor & Francis Group.

Hall, M., & Hearn, J. (2019). Revenge pornography and manhood acts: A discourse analysis of perpetrators' accounts. *Journal of Gender Studies*, *28*(2), 158–170. doi:10.1080/09589236.2017.1417117

Hill, K. (2012, April 5). *Why we find Hunter Moore and his "identity porn" site, IsAnyoneUp, so fascinating*. Forbes. Retrieved from https://www.forbes.com/sites/kashmirhill/2012/04/05/hunter-moore-of-isanyoneup-wouldnt-mind-making-some-money-off-of-a-suicide/

Jane, E. (2018). Gendered cyberhate as workplace harassment and economic vandalism. *Feminist Media Studies*, *18*(4), 575–591. doi:10.1080/14680777.2018.1447344

Johnson, J. J., & Chalmers, K. W. (2007). Identifying employee internet abuse. *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, 247b–247b. 10.1109/HICSS.2007.256

Kelly, L. (1988). *Surviving sexual violence*. Polity Press.

Langlois, G., & Slane, A. (2017). Economies of reputation: The case of revenge porn. *Communication and Critical/Cultural Studies*, *14*(2), 120–138. doi:10.1080/14791420.2016.1273534

Lowry, P., Zhang, J., Wang, C., & Siponen, M. (2016). Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning model. *Information Systems Research*, *27*(4), 962–986. doi:10.1287/isre.2016.0671

Maddocks, S. (2018). From non-consensual pornography to image-based sexual abuse: Charting the course of a problem with many names. *Australian Feminist Studies*, *33*(97), 345–361. doi:10.1080/08164649.2018.1542592

Madigan, S., Ly, A., Rash, C., Van Ouytsel, J., & Temple, J. (2018, April). Prevalence of multiple forms of sexting behavior among youth: A systematic review and meta-Analysis. *JAMA Pediatrics*, *172*(4), 327. doi:10.1001/jamapediatrics.2017.5314 PMID:29482215

McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'revenge porn': The continuum of image-based sexual abuse. *Feminist Legal Studies*, *25*(1), 25–46. doi:10.100710691-017-9343-2

Minc, A. (2017). *Revenge porn law & how to fight back*. Retrieved from https://www.minclaw.com/fighting-back-revenge-porn/

Mohanty, C. T. (1988). Under western eyes: Feminist scholarship and colonial discourses. *Feminist Review*, *30*(1), 61–88. doi:10.1057/fr.1988.42

MooreH. (2012, November 30). https://web.archive.org/web/20121130164110/http://www.huntermoore.tv/

Morris, A. (2012, November 13). *Hunter Moore: The most hated man on the Internet.* Rolling Stone. Retrieved from https://www.rollingstone.com/culture/culture-news/hunter-moore-the-most-hated-man-on-the-internet-184668/

Ophoff, J., Machaka, T., & Stander, A. (2015). Exploring the impact of cyber incivility in the workplace. *Proceedings of the Informing Science Institute*, 493–504. 10.28945/2248

Paul, J. (2015). Workplace cyberharassment: Employer and website operator liability for online misconduct. *North East Journal of Legal Studies*, *33*(1). Retrieved from https://digitalcommons.fairfield.edu/nealsb/vol33/iss1/1

Piotrowski, C. (2012). From workplace bullying to cyberbullying: The enigma of e-harassment in modern organizations. *Organization Development Journal*, *30*(4), 44–53.

Powell, A., & Henry, N. (2017). *Sexual violence in a digital age*. Palgrave Macmillan. doi:10.1057/978-1-137-58047-4

Remove unwanted & explicit personal images from Google—Google Search Help. (n.d.). Retrieved from https://support.google.com/websearch/answer/6302812?hl=en

Richter, F. (2017). *Smartphones cause photography boom* [Digital image]. Statista. Retrieved from https://www.statista.com/chart/10913/number-of-photos-taken-worldwide/

Roy, J. (2012, December 5). *The battle over revenge porn: Can Hunter Moore, the web's vilest entrepreneur, be stopped?* https://web.archive.org/web/20140702082953/http://betabeat.com/2012/12/the-battle-over-revenge-porn-can-hunter-moore-the-webs-vilest-entrepreneur-be-stopped/

Scharr, J. (2015, January 15). *Revenge-porn site shut down by FTC*. Tom's Guide. Retrieved from https://www.tomsguide.com/us/revenge-porn-ftc,news-20383.html

Schwalbe, M. (2014). *Manhood acts: Gender and the practices of domination*. Paradigm.

Starr, T., & Lavis, T. (2018). Perceptions of revenge pornography and victim blame. *International Journal of Cyber Criminology*, *12*(2), 427–438.

Stroud, S. R. (2014). The dark side of the online self: A pragmatist critique of the growing plague of revenge porn. *Journal of Mass Media Ethics*, *29*(3), 168–183. doi:10.1080/08900523.2014.917976

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior*, *7*(3), 321–326. doi:10.1089/1094931041291295 PMID:15257832

Talley v. Chanson. (2014). U.S. Dist. LEXIS 199005, 2014 WL 12167639 (United States District Court for the Southern District of California. May 7, 2014, Filed)

Vera-Gray, F. (2017). *Men's intrusion, women's embodiment: A critical analysis of street harassment*. Routledge.

ViaView, Inc. v. Blue Mist Media, 2012. U.S. Dist. LEXIS 170464, 105 U.S.P.Q.2D (BNA) 1304, 2012 WL 6007204 (United States District Court for the District of Nevada. November 30, 2012, Filed)

Vitak, J., Crouse, J., & LaRose, R. (2011). Personal Internet use at work: Understanding cyberslacking. *Computers in Human Behavior*, *27*(5), 1751–1759. doi:10.1016/j.chb.2011.03.002

Vitis, L. (2019). Private, hidden and obscured: Image-based sexual abuse in Singapore. *Asian Journal of Criminology*, 1–19.

Walker, K., & Sleath, E. (2017). A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media. *Aggression and Violent Behavior*, *36*, 9–24. doi:10.1016/j.avb.2017.06.010

Wilson, O. (2015, June 23). *Revenge porn is more than a violation of privacy it is digital sexual assault*. Huffington Post. Retrieved from https://www.huffpost.com/entry/revenge-porn-is-more-than_b_7641876

YouGov. (2015). *Most commonly regretted types of social media posts according to adults in the United States as of July 2015* [Graph]. Statista. Retrieved from https://www.statista.com/statistics/459369/most-common-social-media-regrets-usa/

Young, K. (2010). Policies and procedures to manage employee Internet abuse. *Computers in Human Behavior*, *26*(6), 1467–1471. doi:10.1016/j.chb.2010.04.025

Young, K., & Case, C. J. (2004). Internet abuse in the workplace: New trends in risk management. *Cyberpsychology & Behavior*, *7*(1), 105–111. doi:10.1089/109493104322820174 PMID:15006175

KEY TERMS AND DEFINITIONS

Clearnet: The world wide web that is accessible via an internet browser. Usually this term is used as a contradistinction to the dark web.

Dark Web: Websites that are only accessible via specialized software and networks. A dark web site's location is obfuscated so it is particularly difficult to apply legal pressure to have non-consensual personal content removed.

Deepfakes: Manipulated media using an artificial neural network to replace a video with someone else's likeness. As computer processing improves, deepfakes will be able to be made by novices with personal computers. Deepfakes can be made of any video genre but are often associated with sexual videos.

Doxxing: To have one's personal information leaked online. This could include one's place of employment, social media accounts, social security number, and family information.

Image-Based Sexual Abuse: An intimate or sexual image shared with a third party non-consensually.

Information Cascade: In this context, this refers to the process of accepting information that others have already shared regardless of what an individual already knows, and then disseminating that information. This forwarding of potentially false or hurtful information makes it difficult to track down the original creators of information.

Non-Consent Fetishization: Fetishizing acts that are done non-consensually. This can include actions such as sexual assault but also attaining and distributing non-consensual photos for pleasure.

Revenge Pornography: The sharing of sexual media with the motivation of harming the person photographed or filmed. While this terminology is commonly used, it is limiting, and many scholars and activists have critiqued its oversimplification of a much larger issue.

Sextortion: A type of image-based sexual abuse whereby a perpetrator threatens to disseminate intimate images or video. This coercion could also be used to blackmail or obtain more images or videos.

This research was previously published in the Handbook of Research on Cyberbullying and Online Harassment in the Workplace; pages 107-128, copyright year 2021 by Business Science Reference (an imprint of IGI Global).