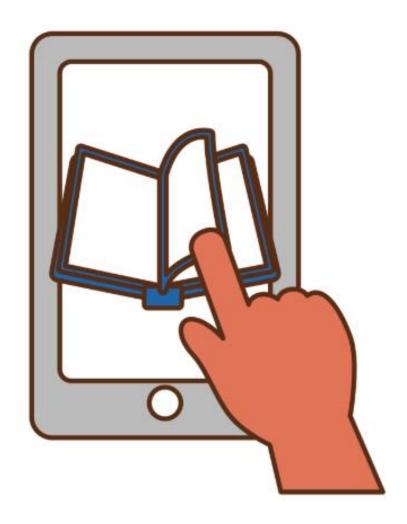
THE CYBER ABUSE PROJECT

Literature Review



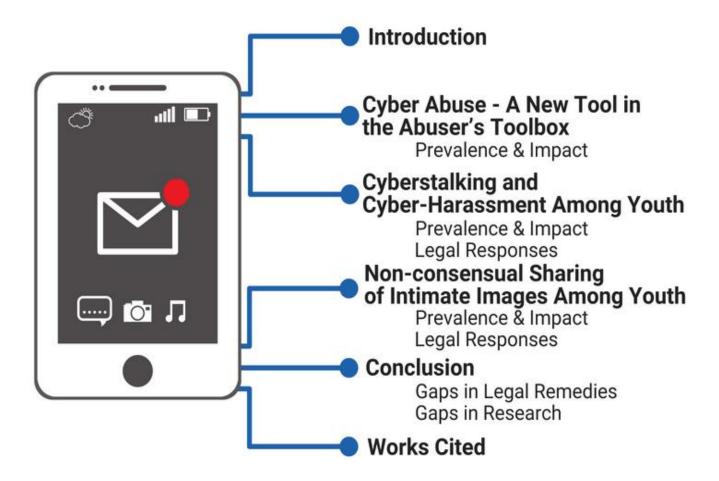
Produced by:



Because Everyone Deserves a Healthy Relationship



TABLE OF CONTENTS



The Cyber Abuse Project was supported by Grant No. 2016-TA-AX-K070 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this program are those of the authors and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

Introduction

With a click of a button and connection to Wi-Fi or a cell phone provider's network, high school and college students can access Facebook to message their friends and family, document their lives in pictures on Instagram, use Snapchat to put funny filters or frames on their photos, or tweet their feelings about whatever is happening in the world. Cell phones and other electronic devices are ubiquitous in young people's daily lives. According to a recent study by the Pew Research Center, 95% of teens have access to a smartphone and 88% have access to a computer.¹ Ninety-two percent of teens report going online daily and 45% report being online "almost constantly."² College students aged 18-24 are the most wide-spread users of the internet, with almost 100% accessing the internet daily, and many (92%) doing so through laptops or cell phones.³

Online interaction has become an important part of youth culture, and young people use the internet to facilitate much of their social interaction. Analyses of digital behavior show that 90% of teens use social media and messaging platforms,⁴ and 86% of college students do so.⁵ Additionally, 88% of college women and 83.4% of college men send text messages daily.⁶ There is also a distinct difference in use of platforms based on socio-economic status and race. Youth from middle and upper income households use Instagram & Snapchat more than youth from lower income households; and African American and Latino youth use messaging apps more than their Caucasian counterparts.⁷ Our connection to technology is simple and the opportunities are vast, but with every new opportunity that technology offers, there is a shadow.

¹ Anderson, M. & Jiang, J. (2018). Teens, Social Media & Technology 2018. Pew Research Center. *Internet and Technology*, 7.

² Anderson & Jiang, 2018, 8.

³ Ranine, L., Smith, A., & Zickuhr, K. (2011, July 19). College Students and Technology. Pew Research Center. *Internet and Technology*.

⁴ Lenhart, A. (2015). Teens, Social Media & Technology Overview 2015: Smartphones Facilitate Shifts in Communication Landscape for Teens. Pew Research Center. *Internet and Technology*, 3.

⁵ Ranine, Smith & Zickuhr, 2011.

⁶ Bennett, D. et. al. (2011). College Students Electronic Victimization in Friendships and Dating Relationships: Anticipated Distress and Associations with Risky Behaviors. *Violence and Victims*, 26, 410-429.

⁷ Lenhart, 2015, 15.

The misuse of technology, or "cyber abuse", is generally characterized as the use of cell phones, computers, and/or other forms of technology to bully, harass, stalk, threaten, or intimidate another person. State and federal laws as well as investigative techniques of criminal justice professionals often have lagged behind new technological developments that enable abusive online behavior. In response to the ongoing prevalence of cyber abuse, the California Coalition Against Sexual Assault and Break the Cycle are working to build the capacity of criminal justice professionals to understand and respond to these issues. In this review, we will discuss the misuse of technology in dating abuse, sexual assault, and stalking situations among youth 12-24, including non-consensual sharing of intimate images, cyber-harassment, and cyberstalking. The review will also address how law and criminal justice professionals. including college and school safety professionals currently respond to these cases. We will also suggest areas where further research would benefit the field. Though cyberbullying, defined broadly as the willful and repeated harm inflicted through the use of technology,8 can overlap with the forms of cyber abuse discussed in this review, it will not be specifically addressed in this literature review.

Cyber Abuse -- A New Tool in the Abuser's Toolbox

Studies have shown a very strong correlation between in-person relationship abuse and cyber abuse. In one of the largest studies to date on the topic, researchers at the Urban Institute examined the digital aspects of teen dating abuse and found that while technology has offered abusers an additional way to degrade, control, and frighten their victims or dating partners, it has not necessarily increased rates of teen dating abuse. Rather, it has created additional methods of abuse and harassment that are perhaps more pervasively and easily employed. Technology is rarely the only way that an abuser inflicts harm; what happens online is often an indicator of what is happening off line between an abuser and a victim. A 2015 study of college students reported in

⁸ "What is Cyberbullying?" Cyberbullying Research Center. 5 June 2017. Retrieved from https://cyberbullying.org/what-is-cyberbullying.

⁹ Zweig, J., & Dank, M. (2013). Teen Dating Abuse and Harassment in the Digital World: Implications for Prevention and Intervention. The Urban Institute. The Urban Institute & United States of America. ¹⁰ *Ibid*.

the *Journal of Interpersonal Violence* showed a nearly one to one correlation between online and in-person abuse: "intimate partner cyber aggression victimization was [found to be] significantly related to in-person experiences of intimate partner psychological, physical, and sexual aggression." More research is needed to determine if experiencing particular forms of abuse through technology signals escalating violence in relationships.

"Technology offers more opportunities for abusers and, unfortunately, the misuse of technology poses additional challenges for investigators and prosecutors who may not be familiar with the types of digital evidence that will be needed at trial."

While cyber abuse is often combined with offline abuse, it clearly poses new investigative and evidentiary challenges for criminal justice professionals, including prosecutors, police, campus safety officials, judges, and advocates. "Technology offers more opportunities for abusers and, unfortunately, the misuse of technology poses additional challenges for investigators and prosecutors who may not be familiar with the types of digital evidence that will be needed at trial." Anderson and Lee point out that digital evidence can live in many different places making it difficult to collect and that forensic software can be expensive. But importantly, they argue that when digital

4

¹¹ Marganski, A. & Melander, L. (2015). Intimate Partner Victimization in the Cyber and Real World: Examining the Extent of Cyber Aggression Experiences and Its Association with In-Person Dating Violence. *Journal of Interpersonal Violence*, 33(7), 1087.

¹² Anderson, J. & Lee, K. (2017, January). The Internet & Intimate Partner Violence: Technology Changes, Abuse Doesn't. AEQuitas. *The Prosecutors' Newsletter on Violence Against Women*, (16),1.

¹³Anderson & Lee 2017, 4.

evidence is combined with offline abuse evidence, it can be a powerful tool for prosecutors and advocates.¹⁴

Prevalence & Impact

Many studies have examined the prevalence of cyber abuse in teen and young adult romantic relationships. One of the earliest was a 2007 study commissioned by Fifth & Pacific Companies, Inc. (formerly Liz Claiborne Inc.) and conducted by TRU (Teenage Research Unlimited). This research provided the first clear evidence that cyber abuse is highly prevalent within teen relationships and that technology has driven abusive conduct underground. More than 1000 teens and parents of teens were surveyed (615 13- to 18-year-olds and 414 parents with teens in that age range). Of those teens who were in dating relationships, the incidence of control and abuse via technology were extremely high. The survey found that:

-

¹⁴ Anderson & Lee 2017, 1.

¹⁵ Picard, P. (2007, January). Research Findings: Tech Abuse in Teen Relationships Study. TRU. Prepared for Fifth & Pacific Companies, Inc., (Formerly: Liz Claiborne, Inc.), 6.

1 in 10 1 in 3 1 in 4 teens who have been in a in a relationship in a relationship relationship 30% 11% 25% Say they've been text say they have been messaged 10, 20, or 30 Report being "textcalled names. times an hour by a checked" by their harassed, or put down partner finding out partners 30 times an by their partner where they are, what hour. through cellphones & they're doing, or who texting. they're with. 1 in 5 1 in 5 teens teens in a relationship in a relationship 22% 19% 18% have been asked via say that their partner say their partner used has used a cellphone cell phone or the a networking site to internet to engage in or the internet to harass or put them sexual activity when spread rumors about down. they did not want to. them. More than 1 in 10 1 in 10 11% 17% 10% say their partner has report that a partner made them afraid not say they have been has shared private or to respond to a cell threatened physically embarrassing phone call, email, IM via email, IM, text, pictures/videos of or text message chat, etc. them. because of what he/she might do. 16%

Figure 1: Data from Picard, 2007

say their partner has actually bought a cellphone or minutes for them.

The research also found that many of these behaviors are used to inspire fear in a partner.¹⁶

Many young people surveyed admitted to participating in cyber abusive behaviors themselves in addition to being victimized by them.¹⁷ Finally, while teens see cyber abuse as a problem, they are not telling their parents about it; the survey revealed major gaps between what teens are experiencing and what parents of teens thought their children were experiencing.¹⁸ Because modes of technology are changing so quickly and access to technology by young people is increasing steadily, updated research is needed on the prevalence of cyber abuse in the relationships of young people and students.

One of the largest cyber abuse studies was conducted in 2013 and surveyed 5,647 youth -- more than any previous analysis -- in 10 northeastern schools.¹⁹ Twenty-six percent of dating teens and eighteen percent of all youth reported experiencing abuse online or through text messages from their partners during the prior year.²⁰

Teenage girls reported higher levels of cyber abuse within a dating relationship (particularly sexual cyber dating abuse, which was twice as high for girls) as well as more cyber-bullying than teenage boys.²¹ In addition, experiencing sexual cyber abuse made victims 7 times as likely to experience sexual coercion within a dating relationship.²² Less than 1 in 10 victims sought help after an incident of cyber abuse, with half as many male

"LGBTQ youth reported significantly higher cyber abuse victimization levels and lower perpetration levels than heterosexual youth."

¹⁶ Picard, 2007, 12.

¹⁷ Picard, 2007, 13-14.

¹⁸ Picard, 2007, 15-22.

¹⁹ Zweig, J. et al. (2013). Technology, Teen Dating Violence and Abuse, and Bullying. Urban Institute Justice Policy Center, pp. iii.

²⁰ Zweig, et al., 2013, iii.

²¹ Zweig, et al., 2013, 4.

²² Zweig, et al. 2013, 33.

victims seeking help as females.²³ LGBTQ youth reported significantly higher cyber abuse victimization levels and lower perpetration levels than heterosexual youth.²⁴ Finally, the study found important risk factors for victimization and perpetration that should be noted by criminal justice professionals and school safety personnel. Youth were at higher risk of cyber abuse victimization if they:

- Were female
- Had committed a high number of delinquent acts
- Had engaged in sexual activity
- Had experienced recent depression, anger, and/or hostility

Factors correlating with perpetration included:

- All of the above factors plus--
- Spending a higher number of hours per day on a cell phone
- More frequent alcohol and/or serious drug use
- Fewer prosocial activities

A 2015 international study conducted by the United Nations Broadband Commission report found that nearly three quarters of women and girls worldwide have experienced some type of cyber abuse, defined broadly as including hate speech, hacking, identity theft, online stalking, threats, induced suicides, and sex trafficking, and

18% had experienced "serious internet violence."²⁵ According to Emily Reynolds of Wired, "[t]he report also found that only 26 percent of law enforcement agencies surveyed were taking appropriate action, [and urged] police forces to take online violence more seriously.²⁶ Professor Nicole Westerland,

"[W]e need to start taking online violence as seriously as abuse that happens in physical spaces, and it may be that this will require further training and investment in policing and prosecuting these forms of violence against women."

8

²³ Zweig, et al. 2013, 52.

²⁴ Zweig, et al. 2013, iii.

²⁵ Reynolds, E. (2015, September 15). UN: 'Urgent Action' Needed on Cyber Violence Against Women. Wired.

²⁶ Reynolds, 2015.

Director of the Durham Centre for Research into Violence and Abuse, commented on the report stating that "[s]ome women receive very little support from the criminal justice system despite a high level of online harassment [...] we need to start taking online violence as seriously as abuse that happens in physical spaces, and it may be that this will require further training and investment in policing and prosecuting these forms of violence against women."²⁷

Two more small but recent studies published in 2016 also found that significant percentages of young people are experiencing cyber abuse within their romantic relationships. One study of 466 secondary school students found that 26% of teenagers in a dating relationship reported being a victim of cyber abuse, defined as "the control, harassment, stalking, and abuse of one's dating partner via technology and social media."²⁸ A 2016 survey of 307 college students who are or were in dating relationships in the past found that nearly 70% had experienced one or more cyber victimization behaviors in the past year and that similar rates existed for women and men.²⁹ However, the study also found that women reported more negative reactions to sexual

"[S]ome of the most common [digital dating abuse] behaviors reported included monitoring a dating partner's whereabouts, monitoring with whom a dating partner is friends and/or talks to, and snooping into a dating partner's private information using digital media."

messaging³⁰ than men.³¹ The study found that "[s]ome of the most common [digital dating abuse] behaviors reported included monitoring a dating partner's whereabouts, monitoring with whom a dating partner is friends and/or talks to, and snooping into a dating partner's private information using digital media.³²

²⁷ Reynolds, 2015.

²⁸ Van Ouystel, J. et al. (2016). Cyber Dating Abuse Victimization Among Secondary School Students From a Lifestyle-Routine Activities Theory Perspective. *Journal of Interpersonal Violence*, pp. 2.

²⁹ Reed, L., Tolman, R., Ward, L. (2016). Snooping and Sexting: Digital Media as a Context for Dating Aggression and Abuse Among College Students. *Violence Against Women*, 22(13), 1564-1569.

³⁰ Sexual messaging refers to sending or receiving sexually suggestive messages including explicit photos.

³¹ Reed, Tolman & Ward, 2016, 1566-67.

³² Reed, Tolman, Ward, 2016, 1564.

Cyberstalking and Cyber-Harassment Among Youth

Cyberstalking and cyber-harassment are common forms of cyber abuse. The terms sometimes are used interchangeably. Cyberstalking however is commonly defined as use of the internet or other electronic means, including email or instant messaging, to stalk another individual. Cyber-harassment on the other hand consists of repeated use of the internet or other electronic means to humiliate, control, or scare another individual.

Cyber-harassment and cyberstalking typically fall into one of three categories: direct communication, indirect communication, and online misrepresentation.³³ Direct communication includes leaving unwanted, harassing messages via email, voicemail, or text message. A common indirect mode of cyber-harassment or stalking includes doxxing or publishing the names, photos, and addresses of targeted individuals with an invitation to harass them. Cyber-harassment or stalking via misrepresentation includes impersonating someone online by hacking into their accounts and/or spreading rumors about them online.

Cyberstalking can take many forms, including surveillance by means of GPS location devices, recording devices installed in a person's home, car, office, or on their phone, posts on a social media site, or emails containing spyware. Spyware can be obtained inexpensively and can

allow an abuser to remotely access a victim's computer, gaining access to their whereabouts as well as information about who they are communicating with and the content of their conversations.

Prevalence & Impact

While research and practice around cyberstalking and harassment have often prioritized adult experiences, young people are particularly vulnerable to these forms of cyber abuse due to their high social media usage rates and relatively newer experience with relationships. Studies show that women may be more susceptible to harm from cyberstalking and cyber-harassment than men.³⁴ Indeed, Danielle Citron -- one of the

³³ Quarmby, K. (2014, August 13). How the Law Is Standing Up to Cyberstalking. *Newsweek Magazine*.

³⁴ Location and Privacy Protection Act of 2014: Hearings before the Subcommittee of the Judiciary on Privacy, Technology, and the Law, Senate Hearing on S. 2171, 113th Congress (2014, June 4) (Testimony of Bea Hanson,

most well known legal scholars in the field -- identifies cyber-harassment as a form of gender discrimination.³⁵ Citron has found that around 60--70% of cyber-harassment consists of sexualized and demeaning content that targets women.³⁶

A major study on stalking, cyberstalking and the difference in stalking prevalence becabetween college students and the general population found that college students are at a higher risk for stalking victimization than the general public (4.3% vs 2.2% during the prior year).³⁷ This study used statistics from the 2006 National Crime Victimization Survey Stalking Victimization Supplement to compare results for college students and non-college students. Importantly, the authors assert that the research makes clear that "most victims of tech-facilitated stalking exist as a smaller subset of victims who experience traditional forms of stalking as well." The study also found that college students report cyber stalking less frequently than non-students. Only 1 in 4

students reported stalking/cyberstalking to the police while 1 in 3 non-college students reported stalking/cyberstalking to police.³⁹ One of the study's authors suggests that students' autonomy, the presence of substance abuse, and the "routine nature of college life" make students more susceptible to stalking and cyberstalking.⁴⁰

"[M]ost victims of tech-facilitated stalking exist as a smaller subset of victims who experience traditional forms of stalking as well."

Principal Deputy Director of the Office on Violence Against Women, U.S. Department of Justice, noting that young women ages 18-24 experience electronic stalking through email, text messaging, and social media at levels well beyond any other demographic group).

³⁵ Citron, D. (2009). Law's Expressive Value in Combating Cyber Gender Harassment. *Michigan Law Review*, 108(3), 375.

³⁶ Quarmby, 2014.

³⁷ Brady, P. & Bouffard, L. (2014). Majoring in Stalking: Exploring Stalking Experiences between College Students and the General Public. Crime Victims Institute College of Criminal Justice at Sam Houston University. *Series on Stalking*, No. 2014-03, 1.

³⁸ Brady & Bouffard, 2014, 2.

³⁹ Brady & Bouffard, 2014, 3.

⁴⁰ Brady & Bouffard, 2014, 1..

The negative impact of cyberstalking on victims is well documented. In a 2008 study of 452 self-identified cyberstalking victims currently enrolled in U.S colleges and universities, several common impacts were found. First, when a victim experiences large quantities of cyberstalking behaviors, the victim is more likely to experience severe psychological side effects, including impaired academic functioning. The study also found that where there was a prior dating or intimate partner relationship, victims reported increased psychological distress. Finally, in the cases of unknown or female stalkers, victims experienced higher rates of poor academic functioning. Most students did not report the victimization to criminal justice professionals or their schools.

A 2012 study of cyber-harassment among college students found that among the 420 undergraduate students surveyed, there was a 43.3% rate of cyber-harassment.⁴⁶ Interestingly, the authors noted that a similar study conducted in 2004 -- eight years earlier -- found an incidence rate of only 16.2%.⁴⁷ Students were at higher risk of experiencing cyber-harassment if they spent more time on social networking sites or had ever sent a sext message.⁴⁸ The authors recommended the development of evidence-based interventions as well as further research into how students cope with cyber-harassment and what percentage report such behavior.⁴⁹

Legal Responses

Many aspects of cyberstalking and cyber-harassment make these forms of abuse easier to engage in and harder to prosecute than traditional offline stalking and harassment cases. First, the perpetrator does not have to be in proximity to the victim. ⁵⁰ The ability to stalk a victim from a different city, state, or country can complicate

⁴¹ Hensler-McGinnis, N.F. (2008). Cyberstalking Victimization: Impact and Coping Responses in a National University Sample, 1-185.

⁴² Hensler-McGinnis, 2008, 145.

⁴³ Hensler-McGinnis, 2008, 144-45.

⁴⁴ Hensler-McGinnis, 2008, 144-45.

⁴⁵ Hensler-McGinnis, 2008, 150-51.

⁴⁶ Lindsay, M. & Krysik, J. (2012). Online Harassment Among College Students: A replication incorporating new trends. *Information, Communication & Society*, 15(5), 703-719.

⁴⁷ Lindsay & Krysik, 2012, 703.

⁴⁸ Lindsay & Krysik, 2012, 703.

⁴⁹ Lindsay & Krysik, 2012, 703.

⁵⁰ Goodno, N.H. (2007). Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws. *Missouri Law Review*, 72 (1), 129.

jurisdictional issues if the victim decides to pursue legal remedies.⁵¹ For example, in the case of the American opera singer Leandra Ramm, Ms. Ramm was unable to stop her Singaporean stalker for years, and his harassment and stalking (including death threats) ruined her career and severely impacted her emotional health. U.S. authorities claimed to have no jurisdiction over her abuser because the crimes were committed "in Singapore," and the Singapore government did not recognize the crime of cyberstalking.⁵² Ms. Ramm found justice in 2013 -- nearly 9 years later -- when her stalker plead guilty in a Singaporean court to, among other charges, sending Ms. Ramm 31 threatening emails.⁵³ This was the first successfully prosecuted international cyberstalking case.⁵⁴

Second, the information that the cyberstalker or harasser shares can spread quickly to other sites, which makes it much harder to permanently remove threats or information from the internet than if the threats were shared verbally.⁵⁵ When someone harasses or abuses another person on a public website, it is easy for other visitors to that site to also harass or abuse the victim, and "cyber-mobs" can result.⁵⁶ This expansion of abuse by others initially unrelated to the cyberstalking or harassment differs significantly from offline stalking behavior⁵⁷ and presents new legal challenges in



"[B]ecause electronic communication can occur at any time, regardless of physical proximity, and with rapid-fire intensity, electronic victimization may be particularly pernicious."

both civil and criminal protection orders, as the protection order usually prohibits conduct by the opposing party or defendant only. As Diana C. Bennett put it, "because electronic communication can occur at any time, regardless of physical proximity, and with rapid-fire intensity, electronic

⁵¹ Lipton, J.D. (2011). Combating Cyber-Victimization. *Berkeley Technology Law Journal*, 26(2), 1113.

⁵² Quarmby, 2014.

⁵³ Quarmby, 2014.

⁵⁴ Quarmby, 2014.

⁵⁵ Lipton, J.D. 2011, 1112.

⁵⁶ Goodno, 2007, 129.

⁵⁷ Goodno, 2007, 129.

victimization may be particularly pernicious".58

Finally, cyberstalking and harassment can also lend the perpetrator anonymity, which removes inhibitions that may prevent someone from stalking or harassing in person and can make it easier for a perpetrator to impersonate the victim online.⁵⁹

As with other forms of online abuse, the law has lagged behind technology in addressing cyberstalking and harassment. However, there has been some significant progress in this arena. On August 1, 2014, the Istanbul Convention became binding in countries that ratified it; the Convention established standards to address gender and domestic violence⁶⁰ and coordinated gender-neutral stalking laws across Europe.⁶¹ Additionally, all states in the United States now have some form of cyberstalking or cyber-harassment laws in place.⁶² These laws can be limited by either jurisdictional issues, as mentioned above, or First Amendment protections, but they still provide a valuable option to victims of cyberstalking.⁶³

For example, the District of Columbia amended its stalking statute to cover stalking by "any means" and to define "any means" as including: "the use of a telephone, mail, delivery service, e-mail, website, or other method of communication on any device. The term "any device" is defined as "electronic, mechanical, digital or any other equipment, including: a camera, spycam, computer, spyware, microphone, audio or video recorder, global positioning system, electronic monitoring system, listening device, night-vision goggles, binoculars, telescope, or spyglass." Clearly, as technology evolves, this list may need to be revisited and amended.

⁵⁸ Bennett, 2011, 411.

⁵⁹ Goodno, 2007, 129.

⁶⁰ Council of Europe. (2018). About the Convention: Historical Background. *Istanbul Convention: Action against Violence Against Women and Domestic Violence*. Retrieved on 20 April 2018 from www.coe.int/en/web/istanbul-convention/historical-background.

⁶¹ Quarmby, 2014.

⁶² D'Amico, M. (2013). FAQ: The Law vs. Online Stalking. Findlaw.

⁶³ Lipton, 2011, 1116.

⁶⁴ D.C. Code § 22-3132(2), (8) (2009).

⁶⁵ D.C. Code § 22-3132(1) (2009).

Non-consensual Sharing of Intimate Images Among Youth

The non-consensual sharing of intimate or private images, commonly known as "revenge pornography", is defined as "the distribution of sexually graphic images of individuals without their consent." These images often are posted online by expartners who previously obtained the images from the victim consensually; though in other cases perpetrators hack into victims' computers or online accounts in order to obtain the images. In some instances, revenge is the motive, but in others it is not, and the perpetrator may not know even the victim. Some perpetrators use the threat to expose a sexual image to control the victim or make them do something they don't want to do such as provide more images or money. This is referred to as "sextortion." Some perpetrators may not explicitly intend to cause harm or embarrassment. Other potential motivations behind the perpetration of this abuse can range from bragging, to arousal, to amusement. Abusers sometimes use explicit images to threaten the victim if they consider leaving the relationship. What these cases have in common is that the image sharing is non-consensual. In this review, we will use the term "non-consensual sharing of intimate images" in order to include each of these potential scenarios.

Prevalence & Impact

Meaningful data on the prevalence, risk factors, consequences of, and experiences of victims of the non-consensual sharing of intimate images is lacking.⁷¹ One small study conducted at Bridgewater State University (BSU) in 2016, which surveyed 167 college students, found that while the prevalence of victimization was low (5 students of 167 had been victims; 3 of whom said the image was posted by a

⁶⁶ Franks, M. (2014, September 7). Combating Non-Consensual Pornography: A Working Paper. *SSRN Electronic Journal*.

⁶⁷ Laird, L. (2013, November). Victims Are Taking on 'Revenge Porn' Websites They Didn't Consent To. *ABA Journal*.

⁶⁸ Wolak, J. & Finkelhor, D. (2016). Sextortion: Findings from a survey of 1,631 victims. Retrieved from Crimes Against Women Research Center & Unviersity of New Hampshire https://27l51l1qnwey246mkc1vzqg0-wpengine.netdna-ssl.com/wp-content/uploads/2016/08/Sextortion Report.pdf.

⁶⁹ Citron, D.K. & Franks, M. (2014). Criminalizing Revenge Porn, Wake Forest Law Review, 49, 349.

⁷⁰ Eaton, A., Jacobs, H., & Ruvalcaba, Y. (2017). 2017 Nationwide Online Study of non consensual Porn Victimization and Perpetration: A Summary Report. Cyber Civil Rights Initiative, Inc., 4.

⁷¹ Eaton, Jacobs, & Ruvalcaba, 2017, 4.

stranger and 2 said by an acquaintance), the impacts were severe.⁷² One of the five students in fact reported harming or considering harming themselves.⁷³ In addition, "[f]our of the five victims reported that the victimization impacted their sense of safety or trust; two identified social difficulties with friends and emotional or sexual problems with current/former romantic or sexual partners. One victim reported academic problems in school and another reported her sexuality being influenced in a positive way."⁷⁴

"This argues for criminal justice professionals who work with student victims to take a victim-centered approach and explore the preferences of the victim with regard to the consequences for the perpetrator."

Interestingly, victims in the BSU study were also asked what they thought the consequences should be for the perpetrator and for the website on which the images were posted. "Two people felt jail or prison, a fine, and expulsion [from school] was appropriate. Two individuals felt that the offender should be forced to pay financial compensation and three respondents felt that

the offender should be forced to undergo counseling. Regarding the website or social media site, one person felt the website should be forced to shut down and its staff responsible for sharing content should be prosecuted and sent to prison. Three respondents felt the website should be given a fine and two respondents felt that nothing should happen to the website." While a small sampling, these varying responses indicate that there may be wide ranging views amongst victims of what the consequences for perpetrators of this type of online abuse should be. This argues for criminal justice professionals who work with student victims to take a victim-centered

⁷² McCue, C. (2016). Ownership of Images: The Prevalence of Revenge Porn Across a University Population. *Bridgewater State University's Master's Theses and Projects*, (43), 57.

⁷³ McCue, 2016, 57.

⁷⁴ McCue, 2016, 57.

⁷⁵ McCue, 2016, 61.

approach and explore the preferences of the victim with regard to the consequences for the perpetrator.

In one of the largest sextortion studies conducted by the Crimes Against Children Research Center and Thorn, responses from 1,631 victims ages 18-25 (many of whom were minors at the time of their experience) found that 60% knew the perpetrator in person before being threatened by them and 40% met their perpetrator online. The study also posited that the threats are real and in 45% of cases, perpetrators carried out their threat to reveal sexual images without the victim's consent. For these 1631 young people, the threat of non-consensual sharing of images caused serious harm with 1 in 4 seeking help from a medical or mental health professional and 1 in 8 moving from their homes for fear of their safety. Many victims did not talk about their abuse with anyone, but 20% reported to tech companies including websites or apps where perpetuation took place, and 16% reported to law enforcement.

When law enforcement was involved, respondents reported barriers including law enforcement's lack of criminal law knowledge, jurisdiction issues, and difficulty identifying perpetrators. "Some also reported being shamed or blamed by police and some who were minors during incidents were threatened with prosecution for producing child pornography." One recommendation of the report was to improve law enforcement's capacity to respond to sextortion cases and to improve their sensitivity to victims.

In some cases where a victim's images are shared non-consensually, perpetrators post the images along with the victim's personal information, such as their name, address, or contact information.⁸¹ They also may post the images along with false information about the victim that invites others to harm the victim. For instance, in California a defendant posed online as a woman who had rejected him and stated that she had violent rape fantasies alongside her address and phone number.⁸² This

⁷⁶ Wolak & Finkelhor, 2016.

⁷⁷ Wolak & Finkelhor, 2016.

⁷⁸ Wolak & Finkelhor, 2016.

⁷⁹ Wolak & Finkelhor, 2016.

⁸⁰ Wolak & Finkelhor, 2016, 6.

⁸¹ Laird, 2013.

⁸² Goodno, 2007, 129.

resulted in at least 6 men showing up at the victim's door with the intent of harming the victim.⁸³

The majority of victims of non-consensual sharing of intimate images are women, and women typically experience more extreme negative outcomes after having been victimized in this way.⁸⁴ The consequences of non-consensual sharing of intimate images for the victim can range from losing one's job, to being harassed, threatened, or even physically harmed by strangers who have seen the image.⁸⁵ Of course serious emotional distress can result as well.

Legal Responses

The research reveals that there is a significant lack of appropriate legal responses and few adequate civil or criminal legal remedies on either the state or federal level to address the non-consensual sharing of intimate images. Many advocates and academics believe it is necessary to criminalize the non-consensual sharing of intimate images. Because the civil remedies discussed below are incomplete in many states, they argue that criminalizing this type of abuse on the state and federal level would both provide another legal option to victims and act as a deterrent to those considering posting non-consensual intimate images online. Additionally, Mary Anne Franks argues that criminalization is the most accurate representation of the harm that this type of cyber abuse creates. Franks argues that the publishing and use of explicit sexual images without the subject's consent is a form of sexual violence despite that the violence does not happen physically to the victim's body.

Authors pushing for criminalization acknowledge the importance of maintaining the freedom of speech granted by the First Amendment. However, they argue that the First Amendment does not protect all types of speech. Academics and advocates have

⁸³ Goodno, 2007, 129.

⁸⁴ Franks, 2014, 4.

⁸⁵ Scheller, S. H. (2015). A Picture is Worth A Thousand Words: The Legal Implications of Revenge Porn. *North Carolina Law Review*, 49(2), 553.

⁸⁶ Castro, D. & McQuinn, A. (2015, July 15). Why and How Congress Should Outlaw Revenge Porn. Information Technology & Innovation Foundation, 5.

⁸⁷ Franks, M. (2013, Feb 15). Why We Need Federal Criminal Law Response to Revenge Porn. *Concurring Opinions*.

⁸⁸ Franks, 2013.

argued that privacy-invading speech without public benefit, such as non-consensual sharing of intimate images, should constitute an exception to First Amendment protection.⁸⁹ Additionally, Citron and Franks argue that many First Amendment arguments reflect a belief that sexual autonomy and consent, especially the autonomy and consent of women, is not as important as other values leading to regulation.⁹⁰ They argue that areas unrelated to sexuality and gender, such as trade secrets, have been regulated without the same level of protest rooted in the First Amendment.⁹¹

Several countries, such as the Philippines, the Australian state of Victoria, Israel, Canada, England and Wales, and New Zealand, have criminalized the non-consensual sharing of intimate images, and other countries are considering criminalization.⁹²

At this time, 40 states and the District of Columbia have laws that criminalize the non-consensual sharing of intimate images, and the number is steadily climbing.⁹³ These laws range from classifying such acts as misdemeanors to felonies



and vary in how they define non-consensual sharing of intimate images. In addition, since January 2017, ten states have enacted laws criminalizing "sextortion" or amended existing laws to encompass the crime of sextortion. An additional group of states, like Washington and Florida, have broad enough laws that already encompass the crime of sextortion. For example, under the Washington code extortion means "knowingly to

⁸⁹ Lichter, S. (2013, May 27). Unwanted Exposure: Civil and Criminal Liability for Revenge Porn Hosts and Posters. *Jolt Digest*, Harvard Law School.

⁹⁰ Citron, D.K. & Franks, M. (2014). Criminalizing Revenge Porn. Wake Forest Law Review, 49, 349.

⁹¹ Citron & Franks, 2014, 349.

⁹² Franks, M. (2016). Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators. Civil Rights Institute, 3.

⁹³ Cyber Civil Rights Initiative. (2018). 40 States + DC Have Revenge Porn Laws. Retrieved from www.cybercivilrights.org/revenge-porn-laws/.

obtain or attempt to obtain by threat property or services of the owner, and specifically includes sexual favors."⁹⁴ Several other states have laws pending, including Washington D.C., that would amend current extortion laws to include the crime of sextortion. Yet, in many states, because sextortion is not codified as a crime, prosecutors either fail to prosecute sextortion or use existing statutes that do not fully capture the nature of sextortion or the extreme harm victims experience.⁹⁵ As a result, there are large disparities in sentencing of sextortion perpetrators, with some cases not being tried as sex crimes at all.⁹⁶

"Many advocates argue that while state criminalization of some types of nonconsesnual sharing of intimate images exists in most states and is an important step, the nonconsensual sharing of intimate images should be federally criminalized."

Many advocates argue that while state criminalization of some types of non-consensual sharing of intimate images exists in most states and is an important step, the non-consensual sharing of intimate images should be federally criminalized.⁹⁷
Criminalization on the federal level would provide uniformity and a model for states to follow.⁹⁸

Federal criminalization also would remove from the victim the financial burden of filing a civil lawsuit, regardless of the state in which she lives, because the government would prosecute the criminal matter and the victim would not be required to obtain legal representation.⁹⁹ Currently, only victims residing in states where the non-consensual sharing of intimate images is a crime have this option. Federal criminalization also

⁹⁴ Wash, Rev. Code § 9A.56,110 (1999).

⁹⁵ Legal Momentum, Thomas Reuters Foundation & Orrick, Herrington & Sutcliffe. (2016). A Call to Action: Ending 'Sextortion' in the Digital Age, 22.

⁹⁶ Wittes, B., Poplin, C., Jurecic, Q. & Spera, C. (2016, May). Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault. Center for Technology Innovation at Brookings, 5.

⁹⁷ Linkous, T. (2014). It's Time for Revenge Porn to Get a Taste of Its Own Medicine: An Argument for the Federal Criminalization of Revenge Porn. *Richmond Journal of Law & Technology*, *XX*(4), 36.

⁹⁸ Linkous, 2014, 36.

⁹⁹ Linkous, 2014, 36.

would provide a consequence for perpetrators who are judgment-proof or unable to pay the fines that result from a civil case.¹⁰⁰

Legislators originally wrote Section 230 of the Federal Communications Decency Act to make it easier for websites to restrict objectionable content while not unnecessarily preventing free speech and expression. 101 Until recently, Section 230 contained two subsections. Section 230(c)(1) prevented internet providers from being held liable for the user-created content that is on their websites, and Section 230(c)(2) prevented internet providers from being held liable for editing or restricting material on their websites. 102

However, Section 230 was recently amended by the Fight Online Sex Trafficking Act (FOSTA) and Stop Enabling Sex Traffickers Act (SESTA), passed by Congress and signed by the President on April 11, 2018.¹⁰³ These amendments to Section 230 remove websites' immunity for third-party postings for prostitution.¹⁰⁴ Authors of the legislation hope it will make it possible to sue sites such as Backpage, which had an active and knowing role in posting ads involving victims of sex trafficking, yet evaded consequences for many years through Section 230.¹⁰⁵

The amendments were controversial and divided the sex work and trafficking activist communities. Some anti-trafficking organizations, such as World Without Exploitation, argue that FOSTA-SESTA holds websites accountable when they are participating in trafficking and offers a way for survivors of trafficking to seek justice. Other anti-trafficking and sex workers' rights organizations believe that FOSTA-SESTA will endanger them. They argue that losing online platforms makes it much more difficult to screen clients, work indoors instead of on the streets, and share information with

¹⁰⁰ Citron, & Franks, 2014, 349.

¹⁰¹ Citron, D.K. & Wittes, B. (2017, July 24). The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity. *Fordham Law Review*, Forthcoming. *University of Maryland Legal Studies Research No. 2017-22*, 5. ¹⁰² Citron & Wittes, 2017. 5.

¹⁰³ Romano, A. (2018, April 18). A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet As We Know It. *Vox.*

¹⁰⁴ Romano, 2018.

¹⁰⁵ Selyukh, A. (2018, March 21). Section 230: A Key Legal Shield for Facebook, Google Is About To Change. National Public Radio. *All Tech Considered*.

¹⁰⁶ Foster, R. (2018, May 3). Effective Lobbying Starts With Listening: How Survivor Voices Drove the Fight for Passage of FOSTA-SESTA. *World Without Exploitation*.

other sex workers about dangerous clients.¹⁰⁷ Sex workers also argue that these changes will negatively impact sex trafficking victims by pushing sex trafficking further underground.¹⁰⁸

In response to the passage of these two bills that amend Section 230 of the Federal Communications Decency Act, Craigslist pulled their personal ads page, and Reddit banned certain subreddit threads. Google Drive has begun to directly review and delete user content. These actions, alongside other responses from websites and servers, point to larger shifts in website management due to FOSTA-SESTA. However, as this bill has passed very recently, it is too soon to know if and how the nonconsensual sharing of intimate images will be impacted.

Despite the wide-ranging consequences, victims, advocates and lawyers have argued that few legal protections exist that mandate removal of intimate images from the internet and penalize the uploaders and/or host websites. 111 A number of different legal strategies have been used to address non-consensual image sharing to varying effect, which we describe below.

Privacy torts are one avenue for redress of the harms caused by non-consensual sharing of intimate images. The approach has its limitations though. Privacy torts were created before the advent of 21st century technology, which magnifies and extends the damage of non-consensual sharing of private images. Because it is so difficult to remove information from the Internet, the injury to the privacy of the victim does not necessarily end after a certain amount of time has passed, and the images reach a much larger audience than was possible before the advent of the Internet. 113

Additionally, the narrow scope of the four main types of privacy torts-- "1) unreasonable intrusion upon a person's seclusion; 2) appropriation of someone's name or likeness; 3) unreasonably giving publicity to a person's private life; and 4) publicizing

¹⁰⁷ McCombs, E. (2018, May 11). 'This Bill is Killing Us': 9 Sex Workers on Their Lives in the Wake of FOSTA. *Huffington Post*.

¹⁰⁸ McCombs, 2018.

¹⁰⁹ Romano, 2018.

¹¹⁰ McCombs, 2018.

¹¹¹ Levandowski, A. (2014). Using Copyright to Combat Revenge Porn. *New York University Journal of Intellectual Property and Entertainment Law*, *3*, 425.

¹¹² Citron, D.K. (2010). Mainstreaming Privacy Torts. California Law Review, 98(6), 1809.

¹¹³ Citron, 2010, 1809

someone in a false light"114-- does not always allow space to address the new types of harm inflicted in the digital age. 115 For instance, if the victim photographed the explicit image and shared it with her partner who then shared it publicly, the unreasonable intrusion tort would not apply as the victim initially chose to share the image. 116 The appropriation of someone's name or likeness tort only applies when the offender uses the name or likeness to personally benefit himself socially or financially, or to boost his own reputation. 117 Because those posting private images do not typically receive benefits in these ways, this tort does not often apply to these cases. 118 A significant barrier in the use of the "unreasonably giving publicity to a person's private life" tort also known as the "public dissemination of private facts tort" is the ability to establish that there was consent between the two parties to share the photos with each other but a lack of consent to publish those photos for a larger audience. 119 Because both the initial agreement and the latter lack of consent are typically unwritten, it is difficult to establish them. 120 The tort of publicizing someone in a false light requires representation of someone publicly in a false or deceptive manner that is also offensive. This can be difficult to prove in cases where an undoctored photograph is posted without false or deceptive accompanying content. In addition, because a plaintiff in a false light case necessarily must provide evidence of offensive and very personal content, many will not choose to proceed on this basis and thereby shed further public light on the content via litigation.¹²¹

Two other tort claims, defamation and intentional infliction of emotional distress, also theoretically could be used in non-consensual pornography cases. However, these torts have their limitations as well. In the case of defamation, it is often possible for a defendant to argue that, since the image is a photograph and therefore presumed

_

¹¹⁴ Citron, 2010, 1809.

¹¹⁵ Citron, 2010, 1809.

¹¹⁶ Porvaznik, P. (2015, July 30). 'It Seemed Like A Good Idea At The Time': Revenge Porn in Illinois -- A Crime with Myriad Civil Components.

¹¹⁷ Levandowski, 2014, 425.

¹¹⁸ Levandowski, 2014, 425.

¹¹⁹ Thomson, M. (2014, March 18). Law and Revenge Porn. *Harvard Civil Rights-Civil Liberties Law Review*.

¹²⁰ Thomson, 2014.

¹²¹ Lipton, 2011, 1136.

¹²² Larkin, P. J. (2014). Revenge Porn, State Law, and Free Speech. Loyola Law Review, 48(1), 57.

accurate, defamation does not apply because it requires that the statement or image presented be false. Additionally, the defendant could argue that anyone who shares a private photograph runs the risk of loss of confidentiality. Privacy torts have not historically addressed breaches of promises of confidentiality, which would offer more protection to victims of the non-consensual sharing of intimate images. The author Paul J. Larkin argues that this would be a reasonable and important evolution for privacy torts to make; however, in the current

Overall, privacy torts have been largely unsuccessful in addressing the non-consensual sharing of intimate images. Authors have argued for the development of new torts that would more appropriately address the harms caused by the non-consensual sharing of intimate images.¹²⁷

moment breaches of confidentiality are not covered by privacy torts. 126

Copyright law provides another way to address the non-consensual sharing of intimate images, and it is important for criminal justice professionals to understand how copyright law can be used to assist victims in removing content from the internet. If the victim is also the person who took the photo, U.S. copyright law can support that person with takedown procedures, the threat of money damages, and civil liability for uploaders and websites. This is because under U.S. copyright law, the person who takes the photo owns the copyright to it -- even if they share that image with another individual. According to some research, over 80% of non-consensual intimate images are "selfies," which would make them eligible for copyright protection.

Thanks to the Digital Millennium Copyright Act, it is not necessary to register one's copyright of an explicit image; instead, "victims need only submit their name and signature; identify the image; and provide links to the infringing material, contact

¹²³ Larkin, 2014, 81.

¹²⁴ Larkin, 2014, 81.

¹²⁵ Larkin, 2014, 83.

¹²⁶ Larkin, 2014, 83.

¹²⁷ Levandowski, 2014, 425-26.

¹²⁸ Levandowski, 2014, 426.

¹²⁹ Levandowski, 2014, 426.

¹³⁰ Levandowski, 2014, 426.

information and written verification that they believe the use is unauthorized."¹³¹ Using copyright does not change the reality that images will show up in other places on the Internet even as they are taken down from one site. However, those websites that ignore takedown notices lose their immunity, and open themselves up to significant lawsuits from and liability to victims. Using

Copyright does not offer a perfect solution to the issue of non-consensual sharing of intimate images, but it may offer victims quicker access to relief than privacy torts while avoiding the limitations of tort law discussed above. Further, by using copyright protections, victims have been able to navigate around Section 230 of the Federal Communications Decency Act as previously drafted, which did not and still does not provide immunity for content that violates copyright laws.¹³⁴

Gaps in Legal Remedies

As noted above, there are several gaps in legal remedies that need to be addressed with respect to the non-consensual sharing of intimate images. The literature makes clear that these gaps could be addressed in several different ways. Federal criminalization of the non-consensual sharing of intimate images would create uniformity across the country and ensure that victims have recourse to the criminal justice system even in states that have not criminalized this conduct. It would also allow victims to have recourse without having to employ an attorney, sometimes at great expense. Tort laws could develop to address the harms that result from cyber abuse, including cyber stalking, cyber-harassment, and the non-consensual sharing of intimate images. The recent changes to the Federal Communications Decency Act may lower the prevalence of non-consensual sharing of intimate images, but it is as of yet too soon to tell.

Gaps in Research

While many studies have been conducted on the prevalence and impact of various forms of cyber abuse on students, gaps continue to exist. Very few studies have resulted in recommendations for prevention of cyber abuse on campuses. And few

¹³¹ Levandowski, 2014, 443.

¹³² Levandowski, 2014, 443-44.

¹³³ Levandowski, 2014, 444.

¹³⁴ Levandowski, 2014, 427-28.

studies include recommendations for interventions by campus law enforcement. One study recommended that universities work collaboratively with counseling faculty, with no reference to reporting to campus law enforcement. ¹³⁵ Campus law enforcement and school resource officers play a pivotal role in addressing the issue of cyber abuse and should be at the forefront of intervention measures.

"Campus law enforcement and school resource officers play a pivotal role in addressing the issue of cyber abuse and should be at the forefront of intervention measures."



Few studies have focused on the experience of youth who identify as LGBTQ (lesbian, gay, bisexual, transgender, queer/questioning) and gender non-conforming. While some studies have found that LGBTQ youth face greater online harassment than their heterosexual peers, more research is clearly needed in this area. Some studies show that LGBTQ and gender non-conforming students encounter the same levels of stalking online as heterosexual, gender-conforming students, but their experiences are not often highlighted in research and do not garner much news coverage.

Likewise, few studies have focused on the prevalence of cyber abuse among students of color and immigrant students or how these communities may be impacted by cyber abuse, including their willingness to engage with the criminal justice system if they are victimized. It is important for colleges and secondary campuses to create a climate that is supportive of LGBTQ and gender non-conforming students, students of color, and immigrant students disclosing victimization including cyber victimization. They

 $^{^{135}}$ Johnson, L.D. et al. (2016). Cyberbullying on Social Media Among College Students. Vistas Online sponsored by the American Counseling Association, Article 3, 6.

¹³⁶ See GLSEN, CiPHR, & CCRC. (2013, July 10). Out Online: The Experiences of LGBT Youth on the Internet. 1-30.

137

Schumaker, E. (2017, April 11). How Some Colleges Put LGBT Students At Greater Risk of Sexual Assault: New Research Suggests that Specific Resources and Inclusive Campuses Help Protect Queer Students. *Huffington Post*.

can do so by offering culturally specific services and training faculty/law enforcement to understand the complexities of working with these culturally specific populations in a trauma-informed manner.

Each of these gaps should be addressed in order to advance efforts to combat cyber abuse on campuses. It is our hope that this project will begin to fill some of these gaps by offering new tools for criminal justice professionals working with cyber abuse victims on campuses across the United States.

Works Cited

- Anderson, M. & Jiang, J. (2018). Teens, Social Media & Technology 2018. Pew Research Center. *Internet and Technology*, 1-20. Retrieved from http://assets.pewresearch.org/wp-content/uploads/sites/14/2018/05/31102617/PI_2018.05.31_TeensTech_FINAL.pdf.
- Anderson, J. & Lee, K. (2017, January). The Internet & Intimate Partner Violence:

 Technology Changes, Abuse Doesn't. AEQuitas. *The Prosecutors' Newsletter on Violence Against Women*, (16), 1-8. Retrieved from

 http://www.aequitasresource.org/The-Internet-and-Intimate-Partner-Violence-Technology-Changes-Abuse-Does-Not-Issue16.pdf.
- Bennett, D. et. al. (2011). College Students Electronic Victimization in Friendships and Dating Relationships: Anticipated Distress and Associations with Risky Behaviors. *Violence and Victims*, *26*, 410-429. doi: 10.1891/0886-6708.26.4.410.
- Brady, P. & Bouffard, L. (2014). Majoring in Stalking: Exploring Stalking Experiences between College Students and the General Public. Crime Victims Institute College of Criminal Justice at Sam Houston University. *Series on Stalking*, No. 2014-03, 1-4. Retrieved from http://www.crimevictimsinstitute.org/publications/?mode=view&item=48.
- Castro, D. & McQuinn, A. (2015, July 15). Why and How Congress Should Outlaw Revenge Porn. Information Technology & Innovation Foundation. 1-9. Retrieved from http://www2.itif.org/2015-congress-outlaw-revenge-porn.pdf?_ga=2.241550722.1080355554.1531501897-658271368.1531501897.
- Citron, D. (2009). Law's Expressive Value in Combating Cyber Gender Harassment.

 *Michigan Law Review, 108(3), 373-416. Retrieved from

 http://repository.law.umich.edu/mlr/vol108/iss3/3.
- Citron, D.K. (2010). Mainstreaming Privacy Torts. *California Law Review, 98*(6), 1805-1852. Retrieved from https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1057&context=c alifornialawreview.
- Citron, D.K. & Franks, M. (2014). Criminalizing Revenge Porn. Wake Forest Law

- Review, 49, 345-391. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2368946.
- Citron, D.K. & Wittes, B. (2017, July 24). The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity. *Fordham Law Review,* Forthcoming. *University of Maryland Legal Studies Research No. 2017-22*, 1-24. Retrieved from https://ssrn.com/abstract=3007720.
- Council of Europe. (2018). About the Convention: Historical Background. *Istanbul Convention: Action against Violence Against Women and Domestic Violence*. Retrieved from http://www.coe.int/en/web/istanbul-convention/historical-background.
- Cyber Civil Rights Initiative. (2018). 40 States + DC Have Revenge Porn Laws.

 Retrieved from www.cybercivilrights.org/revenge-porn-laws/.
- D'Amico, M. (2013). FAQ: The Law vs. Online Stalking. *Findlaw*. Retrieved from https://technology.findlaw.com/legal-software/faq-the-law-vs-online-stalking.html. D.C. Code § 22-3132. (2009).
- Eaton, A., Jacobs, H., Ruvalcaba, Y. (2017). 2017 Nationwide Online Study of non consensual Porn Victimization and Perpetration: A Summary Report. Cyber Civil Rights Initiative, Inc., 1-28. Retrieved from: https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf.
- Foster, R. (2018, May 3). Effective Lobbying Starts With Listening: How Survivor Voices

 Drove the Fight for Passage of FOSTA-SESTA. World Without Exploitation.

 Retrieved from https://medium.com/world-without-exploitation/effective-lobbying-starts-with-listening-ec0b3abc3cc1.
- Franks, M. (2013, Feb 15). Why We Need Federal Criminal Law Response to Revenge Porn. *Concurring Opinions*. Retrieved from https://concurringopinions.com/archives/2013/02/why-we-need-a-federal-criminal-law-response-to-revenge-porn.html.
- Franks, M. (2014, September 7). Combating Non-Consensual Pornography: A Working Paper. SSRN Electronic Journal, 1-17. doi: 10.2139/ssrn.2336537.
- Franks, M. (2016). Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators.

- Civil Rights Institute. 1-15. Retrieved from https://www.cybercivilrights.org/guide-to-legislation/.
- GLSEN, CiPHR, & CCRC. (2013, July 10). Out Online: The Experiences of LGBT Youth on the Internet. 1-30. Retrieved from https://www.glsen.org/press/study-finds-lgbt-youth-face-greater-harassment-online.
- Goodno, N.H. (2007). Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws. *Missouri Law Review*, 72 (1), 125-197. Retrieved from https://scholarship.law.missouri.edu/mlr/vol72/iss1/7/.
- Hensler-McGinnis, N.F. (2008). Cyberstalking Victimization: Impact and Coping Responses in a National University Sample, 1-185. Retrieved from https://drum.lib.umd.edu/bitstream/handle/1903/8206/umi-umd-5402.pdf;jsessionid=1CE3453449DF64005B382B8E6387E5D1?sequence=1.
- Johnson, L.D., Haralson, A., Batts, S., Brown, E., Collins C., Van Buren-Travis, A., & Spencer, M. (2016). Cyberbullying on Social Media Among College Students. *Vistas Online* sponsored by the American Counseling Association, Article 3, 1-8. Retrieved from https://www.counseling.org/docs/default-source/vistas/article_03b0bf24f16116603abcacff0000bee5e7.pdf?sfvrsn=4.
- Laird, L. (2013, November). Victims Are Taking on 'Revenge Porn' Websites They

 Didn't Consent To. *ABA Journal*. Retrieved from

 http://www.abajournal.com/magazine/article/victims_are_taking_on_revenge_porn_websites_for_posting_photos_they_didnt_c.
- Larkin, P. J. (2014). Revenge Porn, State Law, and Free Speech. *Loyola Law Review,* 48(1), 56-117. Retrieved from https://digitalcommons.lmu.edu/llr/vol48/iss1/2/.
- Legal Momentum, Thomas Reuters Foundation, & Orrick, Herrington & Sutcliffe (2016).

 A Call to Action: Ending 'Sextortion' in the Digital Age, 1-57. Retrieved from https://www.legalmomentum.org/sextortion-report
- Lenhart, A. (2015, April 9). Teens, Social Media & Technology: Overview 2015. Pew Research Center. *Internet & Technology*. 1-47. Retrieved from http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015.
- Levandowski, A. (2014). Using Copyright to Combat Revenge Porn. New York

- University Journal of Intellectual Property and Entertainment Law, 3, 422-446.

 Retrieved from https://jipel.law.nyu.edu/wp-content/uploads/2015/05/NYU_JIPEL_Vol-3-No-2_6_Levendowski_RevengePorn.pdf.
- Lichter, S. (2013, May 27). Unwanted Exposure: Civil and Criminal Liability for Revenge Porn Hosts and Posters. *Jolt Digest*, Harvard Law School. Retrieved from https://jolt.law.harvard.edu/digest/unwanted-exposure-civil-and-criminal-liability-for-revenge-porn-hosts-and-posters.
- Lindsay, M. & Krysik, J. (2012). Online Harassment Among College Students: A replication incorporating new trends. *Information, Communication & Society,* 15(5), 703-719. doi: 10.1080/1369118X.2012.674959.
- Linkous, T. (2014). It's Time for Revenge Porn to Get a Taste of Its Own Medicine: An Argument for the Federal Criminalization of Revenge Porn. *Richmond Journal of Law & Technology*, *XX*(4), 1-39. Retrieved from http://jolt.richmond.edu/jolt-archive/v20i4/article14.pdf.
- Lipton, J.D. (2011). Combating Cyber-Victimization. *Berkeley Technology Law Journal*, 26(2), 1102-1156. doi: 10.15779/Z384702.

 Location and Privacy Protection Act of 2014: Hearings before the Subcommittee of the Judiciary on Privacy, Technology, and the Law, Senate Hearing on S. 2171, 113th Congress (2014, June 4) (Testimony of Bea Hanson, Principal Deputy Director of the Office on Violence Against Women, U.S. Department of Justice).
- Marganski, A. & Melander, L. (2015). Intimate Partner Victimization in the Cyber and Real World: Examining the Extent of Cyber Aggression Experiences and Its Association with In-Person Dating Violence. *Journal of Interpersonal Violence*, 33(7), 1071-1095. doi: 10.1177/0886260515614283.
- McCombs, E. (2018, May 11). 'This Bill is Killing Us': 9 Sex Workers on Their Lives in the Wake of FOSTA. *Huffington Post.* Retrieved from https://www.huffingtonpost.com/entry/sex-workers-sesta-fosta_us_5ad0d7d0e4b0edca2cb964d9.
- McCue, C. (2016). Ownership of Images: The Prevalence of Revenge Porn Across a

- University Population. *Bridgewater State University's Master's Theses and Projects*, (43), 1-107. Retrieved from http://vc.bridgew.edu/cgi/viewcontent.cgi?article=1041&context=theses.
- Picard, P. (2007, January). Research Findings: Tech Abuse in Teen Relationships Study. TRU. Prepared for Fifth & Pacific Companies, Inc., (Formerly: Liz Claiborne, Inc.), 1-27. Retrieved from https://www.breakthecycle.org/sites/default/files/pdf/survey-lina-tech-2007.pdf.
- Porvaznik, P. (2015, July 30). 'It Seemed Like A Good Idea At The Time': Revenge Porn in Illinois-- A Crime with Myriad Civil Components. Retrieved from https://paulporvaznik.com/it-seemed-like-a-good-idea-at-the-time-revenge-porn-in-illinois-a-crime-with-myriad-civil-components/9282.
- Quarmby, K. (2014, August 13). How the Law Is Standing Up to Cyberstalking.

 Newsweek Magazine. Retrieved from

 http://www.newsweek.com/2014/08/22/how-law-standing-cyberstalking264251.html.
- Ranine , L., Smith, A., & Zickuhr, K. (2011, July 19). College Students and Technology. Pew Research Center. *Internet and Technology*. Retrieved from http://www.pewinternet.org/2011/07/19/college-students-and-technology/.
- Reed, L., Tolman, R., Ward, L. (2016). Snooping and Sexting: Digital Media as a Context for Dating Aggression and Abuse Among College Students. *Violence Against Women*, 22(13), 1556-1576. doi: 10.1177/1077801216630143.
- Reynolds, E. (2015, September 15). UN: 'Urgent Action' Needed on Cyber Violence Against Women. *Wired*. Retrieved from http://www.wired.co.uk/topic/online-abuse.
- Romano, A. (2018, April 18). A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet As We Know It. *Vox.* Retrieved from https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom.
- Scheller, S. H. (2015). A Picture is Worth A Thousand Words: The Legal Implications of Revenge Porn. *North Carolina Law Review, 49*(2), 550-595. Retrieved from http://scholarship.law.unc.edu/nclr/vol93/iss2/5.

- Schumaker, E. (2017, April 11). How Some Colleges Put LGBT Students At Greater Risk of Sexual Assault: New Research Suggests that Specific Resources and Inclusive Campuses Help Protect Queer Students. *Huffington Post*. Retrieved from https://www.huffingtonpost.com/entry/lgbt-students-sexual-assault_us_58d2abb7e4b02d33b747b4a4.
- Selyukh, A. (2018, March 21). Section 230: A Key Legal Shield for Facebook, Google Is About To Change. National Public Radio. *All Tech Considered*. Retrieved from https://www.npr.org/sections/alltechconsidered/2018/03/21/591622450/section-230-a-key-legal-shield-for-facebook-google-is-about-to-change.
- Thomson, M. (2014, March 18). Law and Revenge Porn. *Harvard Civil Rights-Civil Liberties Law Review.* Retrieved from http://harvardcrcl.org/law-and-revenge-porn/.
- Van Ouystel, J. et al. (2016). Cyber Dating Abuse Victimization Among Secondary School Students From a Lifestyle-Routine Activities Theory Perspective. *Journal of Interpersonal Violence*, 1-10. doi: 10.1177/0886260516629390.
- Wash. Rev. Code § 9A.56.110 (1999).
- Wittes, B., Poplin, C., Jurecic, Q. & Spera, C. (2016, May). Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault. *Center for Technology Innovation at Brookings*, 1-47. Retrieved from https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf.
- "What is Cyberbullying?" Cyberbullying Research Center. 5 June 2017, Retrieved from https://cyberbullying.org/what-is-cyberbullying.
- Wolak, J. & Finkelhor, D. (2016). Sextortion: Findings from a survey of 1,631 victims.

 Retrieved from Crimes Against Women Research Center & Unviersity of New Hampshire https://27l51l1qnwey246mkc1vzqg0-wpengine.netdna-ssl.com/wp-content/uploads/2016/08/Sextortion_Report.pdf.
- Zweig, J., & Dank, M. (2013). Teen Dating Abuse and Harassment in the Digital World: Implications for Prevention and Intervention. The Urban Institute. The Urban Institute & United States of America. Retrieved from https://www.urban.org/research/publication/teen-dating-abuse-and-harassment-digital-world.

Zweig, J., Dank, M., Lachman, P., & Yahner, J. (2013). Technology, Teen Dating Violence and Abuse, and Bullying. Urban Institute Justice Policy Center, 1-185. Retrieved from https://www.urban.org/research/publication/technology-teen-dating-violence-and-abuse-and-bullying/view/full_report.