The Cyber Pandemic:

Exploring the Financial Sextortion of Young Males

Written by

PRASHANTHI RAJANIKANTH

Under the Supervision

of Dr. Harpreet Aulakh

An Honours Project submitted

in partial fulfillment

of the Degree requirements for the degree of

Bachelor of Arts

(Criminal Justice) Honours

Department of Economics, Justice, and Policy Studies

Mount Royal University

Date Submitted:

April 21st, 2023

MOUNT ROYAL UNIVERSITY CALGARY, AB, CANADA

ABSTRACT

As the world grappled with Covid-19, another epidemic emerged in the cyber world in the form of financial sextortion. This organized crime lures and entraps victims who are primarily teenage males and young men. This exploratory study examines the growing trend of male sextortion in the past couple of years through the lens of Cyber Lifestyles-Routine Activities Theory (CLRAT) and the Modus Operandi (MO) of sextortionists. Using a semi-systematic literature review, this study investigates victimization through the key elements of CLRAT: exposure & proximity, target attractivity, and guardianship. There is also an examination of MO in both the possession and extortion stages, as a way to understand offending behaviours. The findings highlight how the interplay between CLRAT & MO explains the susceptibility of young males to victimization. This new wave of sextortion lures young males primarily for financial gains compared to conventional victims who are females targeted through sexual motives. The study explores the existing minor & gendered-focus lens on sextortion, calling attention to the unique challenges financial sextortion poses from a legal perspective, for law enforcement, and for victim services.

LAND ACKNOWLEDGMENT

Mount Royal University rests on Treaty 7, which encompasses the traditional territories of the Siksikaitsitapi (Blackfoot Confederacy), comprised of the Siksika, Kainai, Piikani, and Amskapi Piikani First Nations; the Tsuut'ina First Nation; and the Îyârhe Nakoda, including the Chiniki, Bearspaw, Wesley First Nations. Treaty 7 is also home to the Métis Nation of Alberta, Region III. I acknowledge the complex history that has allowed settlers, such as myself, to reside on this land, where I am grateful to live, learn, and work. I acknowledge the First Nations, Metis, and Inuit people with the utmost appreciation for their rich cultures and their resilience throughout history.

ACKNOWLEDGMENTS

My first and most earnest acknowledgment goes to Dr. Harpreet Aulakh. Thank you, Harpreet, for being a truly memorable professor from day 1. My acceptance into the honours stream was not initially guaranteed, however, Harpreet believed in me, and took me on with the utmost support and guidance. I would also like to thank Professors Doug King, Ritesh Narayan, and Tracey Lowey for not only growing my interests & shaping how I see the world, but also for their encouragement, support, and kindness throughout my journey in the criminal justice program. I'd like to express further gratitude for the staff at Riddell Library & Learning Centre; working with them has been a highlight of my undergraduate journey, as they have not only provided exceptional academic assistance but most importantly, many of the staff have become my friends. Finally, I wish to acknowledge my family: my younger siblings whom I will always protect, my parents whom I will always love, and my dog, whom I will always play with.

I dedicate this study to survivors of all forms of sexual violence, particularly those who live in silence, or whose pain was never deservedly acknowledged when they came forward. Their woes do not determine their identity. Rather, they are the embodiment of courage and strength in my eyes.

To everyone I have mentioned above, I wish you nothing but goodness.

Table of Contents

The Cyber Pandemic: Exploring the Financial Sextortion of Young Males

The emergence of the coronavirus (Covid-19) pandemic produced an onset of restrictions, lockdowns, and a significant shift toward a digital era. In a time of social distancing, individuals increasingly became cyber-focused and turned to the online world (cyberspace) for entertainment, connection, and support through the adverse times of lockdowns (Nabity-Grover et al., 2020; Eaton et al., 2022). A notable contribution of cyberspace is its role in enhancing social connectedness, which is the sense of belonging and subjective psychological bond that people feel in relation to others (Haslam, et al., 2015). Cyberspace formulates a comfortable environment to engage in online communication, a behaviour that stimulates the personal disclosure of information, explained by the internet-enhanced self-disclosure hypothesis as enhancing relationship quality (Luo & Hancock, 2020). The social connectedness constructed from online personal disclosure is linked to positive well-being in some users (Haslam, et al., 2015). However, aside from some positive benefits, there are growing concerns about the negative implications that arise as a result of certain cyber interactions & online self-disclosures. An escalating concern is the crisis of online exploitation.

As communities prepared to guard themselves against a virus of the physical world, little was known about a hidden pandemic emerging behind screens. Cyberspace has become an oasis for those who utilize the characteristics of the digital environment to exploit the self-disclosure & interactions of users. In recent years, Covid-19 has been a driver of cyber-criminal activity, aided by the impact of school closures, a shift to online learning, work-from-home lifestyles, and a push towards social distancing (Eaton et al., 2022). This has drastically increased the online presence of people, particularly those between the ages of 15-34 (Bilodeau et al., 2021). Higher levels of online exposure have placed people vulnerable to cyber exploitation, such as online grooming, digital harassment, and an exponentially growing crime known as sextortion (Pollard & Kuznar, 2022).

Research Question

The research question explored in this project was, how does the interplay between Cyber Lifestyle-Routine Activities Theory (CLRAT), and the Modus Operandi (MO) of sextortionists, place young males susceptible to victimization in financial sextortion?

CLART is an integrated theory that is combined with Routine Activity Theory (RAT), and Lifestyle Exposure Theory (LET) to explain cyberspace victimization. In the first section of the literature review, CLRAT is applied as a theoretical framework to explain the victimization of young males in financial sextortion. This is followed by a discussion of offender behaviours in order to examine the MO of financial sextortionists. By studying both victimization through CLRAT, and criminal behaviours through a look at MO, this research project provides insight into the crime, and answers why this specific population (young males) is susceptible to victimization.

Methodology

This present study uses "children" in the context of Article 1, of the United Nations Convention on the Rights of the Child, referring to every human being under the age of eighteen years (Convention on the Rights of the Child*,* 1989). Along with minor male victims, who are victimized by financial sextortion, males above the age of 18 are also addressed with importance in this study, since they are the primary victims. Both groups are coined together and addressed as "young males."

An exploratory research design was utilized in this study with the purpose of exploring the novice trend of victimization among young males by financial sextortion. Their victimization is explained through the theoretical framework of CLRAT & its key concepts: exposure, proximity, target attractiveness, and guardianship. Proximity & exposure are analyzed as one concept, rather than as separately. This is due to these concepts frequently sharing common measures in the studies utilizing this theory (Reyns et al., 2011; Vakhitova et al., 2019; Holt & Bossler, 2009).

The objectives of an exploratory research design are to apply concepts, explanations, theories, and hypotheses to a new phenomenon, with the expectation of proposing new ways of understanding its causation and organization (Reiter, 2017). An exploratory research design was chosen in order to examine how much & how well CLRAT, and offender MO explain financial sextortion from both a victimization, and offender approach.

The comprehension of victimization and MO is executed through the incorporation of a semi-systematic literature review into the research design. The literature review is conducted through a qualitative approach that utilizes secondary data collection. The viewing of existing research is significant as this not only explains the crime, but also offers an understanding of the legal limitations of Canada's response to sextortion, the indeterminate legal definition of sextortion, investigatory barriers, the heavily understudied nature of male victimization, lack of adequate victim resources, and the uncertainty of reporting on social media that is prevalent among victims.

Data Collection

A semi-systematic literature review was conducted in order to synthesize research from different fields; the collected data is a part of cyber-psychology, sociology, and cyber-criminology. This allowed the identification of themes, theoretical perspectives, and theoretical models such as CLRAT to be applied (University of North Dakota, 2023). Through discussions, the literature review begins by examining the formation and debates surrounding CLRAT, its key concepts, and how these concepts account for the victimization of young males in financial sextortion. The literature review reveals the integration of exposure & proximity as one concept, while the other three remain the same. The second section of the literature review is followed by an examination of MO in cases of financial sextortion victimizing young males. Common offending behaviours of financial sextortion cases are examined, leading into a further discussion of offending behaviours in both the possession and extortion stage of the crime.

By analyzing CLRAT's capacity to explain financial sextortion, with an examination of MO, this study provides a significant step in enhancing the knowledge of the crime from the stance of both victimization & offending behaviours.

The initial stages of data collection are composed of specific search terms such as "sextortion trends", "pandemic cyber-crimes", "sextortion in Canada", and "sextortion victims." More advanced search terms involved the use of "and" "of" & "in" between words, and lengthier terms such as "online sexual violence", "theories of cyber-sexual crimes", "financial sextortion", "cyber theories of online crime" and "global sextortion schemes."

The primary databases relied upon for this study included the Mount Royal University Library database, Google Scholar, Government of Canada Open Data Portal, Academia.edu, PUBmed National Library of Medicine, ScienceDirect, JSTOR, Canadian Centre for Child Protection Inc., and ProQuest Central.

Data collection was conducted with a plan to avoid confirmation bias, which is the interpreting of evidence in ways that are partial to the researcher's existing beliefs, expectations, or hypotheses (Nickerson, 1998). To prevent the risk of confirmation bias, the research considered all evidence available. This meant seeking out different perspectives regarding victim experiences, uncommon, non-pattern associated MOs, and a search for how different organizations interpreted sextortion. An inclusion/exclusion criterion was implemented in this study, in which the main data was limited to peer-reviewed journal articles, scholarly resources published by educational institutions, and grey literature, consisting of organizational reports, and government documents. Newspaper articles were included to obtain information that was more specific about victim experiences. The research excluded opinion pieces that lacked peer-reviewed or academic sources, one-sided viewpoints, negative language use, and promotion of political ideas. Due to the transnational nature of financial sextortion, the literature review is composed of data from a global perspective. However, discussions of legal documents & statutes are in the Canadian context. The data collection methods of this study were crucial to gathering insight into a phenomenon so understudied. By reviewing various sources, and utilizing different databases, a useful understanding of financial sextortion was obtained.

Significance & Purpose of the Study

Rising records of victimization are noted across Canada, as CyberTip receives an average of 200 sextortion reports per month. Of these reports, 87% affected boys (Canadian Centre for Child Protection [C3P], 2022). Young males in Canada are targeted across different provinces, with Southern Alberta seeing over 100 young male victims from March 2022 to December 2022 alone (ALERT, 2022). From an international comparison, similar numbers are also skyrocketing in India (Kajal, 2022), a nation that witnesses more than 500 cases of sextortion daily, of which only a small percentage are reported (Yadav, 2022). This global crisis is also on the rise in the United Kingdom, as their revenge porn helpline numbers doubled within a year, seeing 1,124 cases of sextortion in 2021, up from 593 reports in 2020. Of these instances, a striking 88% involved male victims (Shaw, 2022). A rise in financial sextortion has also been noted in the

United States. Reports to the National Center for Missing and Exploited Children saw sextortion numbers more than double between 2019 and 2021, and a shift in the dominant motive of offenders from pursuing more explicit images, to seeking money in 2021 (National Center for Missing and Exploited Children [NCMEC], 2023). This global increase in financial sextortion is related to the pandemic, noticed by how 75% of Canadians 15 and older engaged in online activities more often since the onset of Covid-19 (Bilodeau et al., 2021). This is in correspondence with school closures, a shift to online learning, work-from-home/hybrid lifestyles, and a push towards social distancing which peaked during lockdowns. Significant growth in online exposure places people vulnerable to online exploitation of various ways (Pollard & Kuznar, 2022), particularly in the rise of digital extortion offences by 78% from 2019 to 2020, and by 18% from 2020 to 2021 in Canada alone (Moreau, 2022). The increase in online victimization is expected to remain, if not worsen. Researchers from the Pew Research Center predict that people's relationship with technology will deepen as larger segments of the population increase their reliance on digital connections for work, education, healthcare, commercial transactions, and essential social interactions (Anderson et al., 2021). It is crucial to spread awareness and open discussions about a crime that is rapidly spreading, particularly with the overrepresentation of certain groups.

By exploring a comparatively new theme of sextortion that varies in victimization patterns & MO from traditional themes of sextortion, this study is an effort into opening the door to discussions on male victims in Image-Based Sexual Abuse (IBSA) & Technology-Facilitated Sexual Violence (TFSV). IBSA describes offences in which "sexually explicit images or videos are non-consensually produced, manufactured, or distributed" (McGlynn et al., 2017, as cited in O'Malley, 2023, p. 2), whereas TFSV refers to when sexually aggressive behaviours are perpetuated with mobile and online technologies, in order to blackmail, control, coerce, harass, humiliate, objectify, or violate another person (Henry & Powell, 2016; Henry & Powell, 2018). Much of the research in these crime categories have created a gendered discourse where women & girls are extensively included in the debate, and the digital experiences of male victims are excluded. Such gendered discourse perpetuates not only double standards (Kormazer et al., 2020), but limits discussions on why certain groups are susceptible to becoming victims of specific crimes. When victimological knowledge is limited in the unprotectedness of some groups, we eventually fail to understand the crime in its entire context. An error such as this inhibits research on the complacency of authorities, as well as on the explanations surrounding overrepresentation, and victim services.

By creating awareness of the unstructured ways sextortion manifests itself, the present study not only raises awareness on safe-cyber use but also promotes a diverse victim-centered approach that acknowledges victims who are typically excluded from the discussion. By doing so, research gaps are addressed regarding the misconceptions surrounding sextortion, the under-protection of non-conventional victims, and the gross miscarriages of justice that arise from a crisis that is so loosely defined in legal systems.

Sextortion

Sextortion is a type of extortion involving both a sexual and corruption component. It is the deviant act of threatening to expose or distribute sexually explicit materials unless a victim complies with the demands of the perpetrator (also referred to as the sextortionist) (Eaton et al., 2022). Victims first encounter an explicit request to engage in sexual activity, such as exposing private body parts, posing for sexual photographs, or participating in phone sex (International Association of Women Judges [IAWJ], 2012). The victim’s compliance is immediately followed up by threats to distribute their explicit material. A sextortionist will traditionally demand additional explicit material from the victim, sexual favours in person, or their demands are financially motivated.

As a cyber-attack, the seriousness of sextortion falls into the category of both IBSA, and TFSV. Crime such as revenge pornography, nonconsensual distribution of explicit images, cyber-bullying, and cyber-stalking are typically covered under both these categories, however, sextortion is unique, as it is one of the only offences where the explicit material may never be distributed. Victimization still occurs regardless of whether or not the explicit content is shared (O'Malley & Holt, 2022).

Possession is an element of sextortion that introduces sexuality & control to the interaction between victim & offender. Possession of the material, regardless of how it was obtained, also gives the offender an advantage in reinforcing extortion. Extortion is the second element that highlights the power & control yielded by the sextortionist from *possibly* causing harm to the victim. This is key to what differentiates sextortion from other offences of IBSA & TFSV, as the mere *possibility* of harm enhances high emotions of uncertainty, fear, and desperation in the victim, leading to severe psychological torment (Arca, 2016) and often quick decision-making.

Sextortionists breed fear in their victims from the mere threat of distributing the explicit material. Victims' feelings of fear, helplessness, hopelessness, shame, humiliation, and self-blame (Nilsson et al., 2019) are all capitalized upon in order to gain compliance. The seriousness of sextortion does not only fall under IBSA & TFSV, but it also overlaps with Child Sexual Exploitation (CSE) when victims are minors, and Child Sexual Abuse Material (CSAM) is involved. Research notes that minors are particularly vulnerable to sextortion (Europol, 2017;

C3P, 2022; Ibrahim, 2022; Wittes et al., 2016; Patchin & Hinduja, 2020), which places a large volume of sextortion research to focus on underage victims. When sextortion is in the spotlight, oftentimes a child is involved. Sextortionists who harbour sexual interest in their victims, particularly minor victims, tend to dominate the discussions of this crime, which has rendered financial sextortion to be of little discussion.

Traditional Themes of Sextortion

An interesting study by O'Malley & Holt analyzed 152 media articles & court documents and uncovered four different themes of sextortion offenders based on crime characteristics: minor-focused cyber sextortion offenders, cybercrime cyber sextortion offenders, intimately violent cyber sextortion offenders, and transnational criminal cyber sextortion offenders (O'Malley & Holt, 2022). It is important to briefly touch on the various types of sextortion that exist, in order to understand the complexity of this crime regarding the different forms of victims and motives.

Minor-focused cyber sextortion offenders demonstrate a preference for victims under the age of 18, and they demand additional sexually explicit material or physical sexual contact from victims (O'Malley & Holt, 2022). These offenders' prevalence to possess & view CSAM, and their use of grooming techniques toward children, points to the likeliness of their primary motive being a sexual attraction to minors (O'Malley & Holt, 2022). Most of these child sexual predators target strangers, and victim preferences are overrepresented by girls.

Cybercrime cyber sextortion offenders utilize computer-based tactics to obtain explicit images of victims as leverage in their sextortion. Although they overwhelmingly target female victims, they have no preference or sexual interest in minors, nor do they employ grooming tactics. These offenders utilize social engineering strategies such as hacking, or further advanced computer skills in malware (O’Malley & Holt, 2022).

Intimately violent cyber sextortion is similar to traditional forms of intimate partner violence. These perpetrators use explicit images of victims to control their behaviour, and females constitute the majority of victim numbers. The most common demands in intimately violent cyber sextortion are for nonsexual behaviour from victims. These include demands such as remaining in abusive relationships, giving up custody of pets or children, isolating from new relationships & loved ones, or terminating their employment (O’Malley & Holt, 2022). Intimately violent cyber sextortion bears a close similarity to domestic violence; therefore, victims are not chosen randomly. This differentiates this theme from most forms of sextortion.

Transnational criminal cyber sextortion offenders are part of financially motivated, international criminal organizations. These sextortionists hold no preference for victim age, and they have purposefully targeted successful people, such as politicians, and businessmen (Goudie et al., 2016, as cited in O’Malley & Holt, 2022). They utilize webcam scams, and impersonation techniques to trick victims into self-generating explicit material, and they capitalize on time-sensitive demands & heightened emotions (O’Malley & Holt, 2022). This theme of sextortion bears the closest similarity to the financial sextortion that is investigated in the present study. What differentiates transnational criminal cyber sextortion from the new trend of financial sextortion lies in the overrepresentation of young male victims, and the MOs in place, which are explored further.

Financial Sextortion of Young Males: A New Trend of Crime

Financial sextortion is a unique and growing theme of sextortion that occurs when a sextortionist threatens to distribute a victim’s intimate images or videos unless their financial demands are met (O'Malley, 2023; Royal Canadian Mountain Police [RCMP], 2023; C3P, 2022). Often operating from overseas, financial sextortion is a transnational organized activity (ALERT, 2022), run by sextortion rings that are wanted by international police groups (INTERPOL, 2022).

This crime is different from conventional sextortion themes, in that while sextortionists use sex to lure and entrap victims, their demands are strictly financial, and a majority of victims are adult males between the ages of 20-39, and underage boys (O'Malley, 2023). The overrepresentation of male victims is unique from the traditional forms of IBSA & sextortion which primarily victimize females (O'Malley, 2022; C3P, 2022; O'Malley, 2023; Federal Bureau of Investigation [FBI], 2019; Henry & Powell, 2018). The victimization of teenage boys and less financially well-known young men is also different from how transnational criminal cyber sextortionists have conventionally targeted successful people, such as politicians, and businessmen (Goudie et al., 2016, as cited in O'Malley & Holt, 2022).

As an immensely understudied phenomenon, the key findings of financial sextortion reported in this study are aided by the Canadian Centre of Child Protection's (CP3) 2022 analysis of financial sextortion victim posts that were published on reddit.com/r/Sextortion (hereafter referred to as C3P report). The C3P report was created in February 2020 and is one of the largest financial sextortion discussion/support forums on the internet. Reddit users in this community post about their victimization and offer advice & support to each other (C3P, 2022). The C3P report is a primary source of data for this study due to its in-depth analysis of victim narratives & trends, as this provides a more timely and efficient way of understanding the crime.

The CP3 report notes that 60% of victims were 18 or older and 40% were minors when they were victimized. Among these numbers, there was an overrepresentation of male victims by

98% (C3P, 2022), which has also been noticed by law enforcement, who state that although financial sextortionists targets young persons, the most significant increase in victimization involves males above the age of 18 (ALERT, 2022). This suggests that minors are not the primary targets of financial sextortion, however, they are still among the victims (Europol, 2017).

According to the CP3 report, the most frequent platforms used to facilitate financial sextortion tactics were Instagram & Snapchat, followed by WhatsApp, Facebook & Tinder (C3P, 2022). The commonality between these instant messaging applications is that they allow users to exchange messages, photographs, and audio & video messages. In some cases, victimization can occur on more than one social media platform as well. For example, victims can experience initial contact on Instagram and then have the conversation migrate to Snapchat or another chat-based application that allows the distribution of images or videos. Most conversations between victims & sextortionist migrate to Snapchat due to the app's reputation as a sexting application. This is because Snapchat allows messages to be deleted from the company's servers, and from the chats of the engaged accounts (Poltash, 2013).

Once victims face the demands of the sextortionist the crime either proceeds with the victim's compliance or noncompliance. When victims complied with the demands, 93% of cases involved the sextortionist increasing their demands by asking for more money (C3P, 2022); from the assumption of demands in U.S dollars, in the self-reported incidents, most victims were demanded to pay between $100 - $500 (C3P, 2022), however due to underreporting & the hidden true proportion of victims, payment numbers may be higher.

The financial motive behind sextortionists is recognized by their reaction to the victim's compliance or noncompliance. In 60% of cases where victims complied, the sextortionist did not follow through on their threats of distribution and left the victim alone after their financial demands were met. Meanwhile, 30% of sextortionists followed through with their threats after receiving payment. Compared to those who complied, those who did not comply faced a similar likelihood of having their images distributed. 70% of victims who ignored the demands of the sextortionists did not have their images distributed (C3P, 2022). This is interesting to note as it displays financial motive. The similar likelihood of threats being met between a victim who complies and one who refuses to comply shows that most financial sextortionists are quickly victimizing individuals based on the likelihood of obtaining money. The goal of a financial sextortionist is to obtain a financial reward, their likelihood of leaving a victim alone depends on whether or not they will reach that goal. This is why a majority of sextortionists are repeat offenders, have large victim pools, and quickly move on from victim to victim.

An Indeterminate Understanding of the Problem

The unique trend regarding the financial sextortion of young males has so far been dramatically understudied. Sextortion is acknowledged by law enforcement, private advocates, and some government agencies, however, no government agency publishes data on its prevalence alone. The subject lacks academic literature in the areas of victimology, and offender behaviours, and very few legal actions are in place to target the uniqueness of sextortion. Rather, a patchwork of legal measures is relied upon for convicting offenders, with disparities in the treatment and acknowledgment of different types of victims.

One of the biggest challenges that hinder the understanding of sextortion is how it is not a crime in any country (Wittes et al., 2016). The crime’s lack of a legal definition, and unsatisfactory investigative responses have created inadequate protection for victims and produced disparities in legal consequences. Existing literature on the subject has also perpetuated a mainstream victimological viewpoint of sextortion through a gender-based violence lens, as well as a heavy focus on underage victims (O’Malley, 2023; France, 2022; Henry & Powell, 2018). This has produced research gaps, thus contributing to a failure in understanding that IBSA & TFSV can impact both males and females in different ways.

Legal Gaps

There are no specific statutes that target the themes of sextortion, such as its features of a cyber-attack, interpersonal violence, or pedophilia (O’Malley & Holt, 2022). Such a weak legal understanding of the subject diminishes consistency in the prosecution of sextortion cases, leading them to be processed under a hodgepodge of provincial and federal laws (Wittes et al., 2016).

Under Canadian federal law, sextortion is often prosecuted under various Criminal Code provisions such as extortion (Criminal Code, RSC 1985, c C-46, s 346(1)), the non-consensual distribution of intimate images (Criminal Code, s 162(1)), criminal harassment (Criminal Code, s 264(1)), harassing communications (Criminal Code, s 372(3)), uttering threats (Criminal Code, s 264.1(1)), and intimidation (Criminal Code, s 423(1)). With the involvement of victims under the age of 18, child pornography laws are also enacted for making (Criminal Code, s 163.1(2)), distributing (Criminal Code, s 163.1(3)), possessing (Criminal Code, s 163.1(4)), and/or accessing child pornography (Criminal Code, s 163.1 (4.1)).

Canadian provincial governments have also addressed similar crimes through their own legislation, such as Alberta’s Protecting Victims of Non-Consensual Distribution of Intimate Images Act, the Saskatchewan Privacy Act, Manitoba Intimate Images Protection Act, Nova Scotia’s Intimate Images & Cyber-protection Records Act, and the Newfoundland & Labrador Intimate Images Protection Act (Reclaim Pro Bono, 2022). A comparison of Canadian legal protection in sextortion to those of other countries, shows that some countries only criminalize sextortion that is financially motivated while others criminalize it when there is a legal framework for gender-based violence or the involvement of minors (France, 2022).

In comparison to other legal frameworks covering sextortion, Canada is on the correct track, however, the response of the Canadian criminal justice system could ameliorate. Under anti-corruption frameworks, very few legislations cover the complex nature of sextortion surrounding its elements of extortion & possession together which differentiates it from traditional IBSA & TFSV (O'Malley & Holt, 2022). Law enforcement officials in Canada & around the world also continue to rely on a patchwork of criminal legislation that does not cover the entirety of ways in which sextortion manifests itself (France, 2022), such as financial sextortion, in which victimology is unique from the conventional view of sextortion. New laws are needed in order to specifically target the complex nature of all types of sextortion.

Disparities in Legal Consequences

Despite legal efforts in place to apprehend sextortionists, there exists an under-protection of victims. While prosecutors can rely on a patchwork of criminal legislation to provide consequences to a sextortionist, an assortment of charges produces disparate sentences (Wittes et al., 2016).

Another challenge that has produced disparities in sextortion's legal consequences are investigative challenges. Victims' delays in reporting and lower availability of case information as compared to physical assaults contribute to investigative challenges (Rotenberg, 2017, as cited in Ibrahim, 2022). However, when victims do come forward and information is available, not all cases obtain adequate justice, particularly for adult victims. Sentencing is lighter when the victim is an adult, therefore limiting prosecutors from using child pornography statutes. This is an impudent way of treating adult victims of IBSA, something which is highly prevalent among victims of financial sextortion. The involvement of children raises more severe legal consequences, whereas victims over the age of 18 face less support in the justice system. This study does not doubt that child exploitation cases should be treated with heavy severity. That said, sextortion incidents with adult victims primarily tend to be prosecuted as hacking or extortion offences, instead of as sexual abuse focused crimes. This disparate treatment of adult & minor victims creates an under-protection of those of either gender, who are coerced or manipulated into producing explicit images (Wittes et al., 2016).

An argument that authenticates this disparity says that adult pornography is protected as freedom of expression, whereas child pornography is a form of exploitation & violation. CSAM is indeed exploitative material, however, the disparate treatment of adults & children results in a gross miscarriage of justice as a result of the under-protection of adult victims who are coerced or manipulated into producing pornography by their offender.

Sextortion charges are more likely to be laid when incidents involve multiple criminal code violations, thus creating disparities in legal consequences for offenders. Even in the presence of minor victims, between 2014 and 2020, 56% of police reported online child sexual offences were not cleared by police, meaning an accused was not identified. Incidents involving at least one other criminal code violation are much more likely to be solved but depending on the type of violation. For example, invitation to sexual touching has the highest charge rate in Canada. However, non-consensual distribution of intimate images offences are least likely to lead to charges due to its occurrence in cyberspace. This is a result of the investigatory obstacles present in cyberspace, such as anonymization techniques, which typically presents less evidence (Ibrahim, 2022).

Investigative obstacles, and inadequate legal frameworks limit victims of financial sextortion from obtaining justice. This study advocates for better protective and reactive measures surrounding victims, particularly of less recognized victims such as males & adults.

Mainstream Lens on Victimology

Most research on IBSA & TFSV and sextortion has been influenced by the feminist perspective, and this has centered the discussion of victimology on predominantly women and children (France, 2022; O'Malley & Holt, 2022; Wittes et al., 2016; Patchin & Hinduja, 2020; Champion et al., 2022).

Henry & Powell (2016) claim that TFSV is a gendered phenomenon since women and girls are the main targets of online digital sexualized violence, and because sexual violence in 'offline' contexts, disproportionately victimizes women and girls (sexual harassment, domestic violence, and sexual violence). The consideration of offline sexual violence against women may also influence this gendered lens due to the higher prevalence of women reporting interpersonal & sexual victimization than men (Eaton et al., 2022; Roebuck et al., 2020). Other researchers such as Holt & Bossler (2009) have noted that being female increases the odds of victimization to cyber-harassment when spending more time in a specific online setting. This is also noticed among Franklin (2014) who states that females are overrepresented in some interpersonal violence-related IBSA, such as revenge pornography. Significantly females are preferred targets in sextortion when motives are primarily sexual, with demands for additional explicit material (O'Malley & Holt, 2022; C3P, 2022), and their victimization proves severe impacts. That said, an emphasis on women-centered IBSA & TFSV overshadows the experiences of male victims, particularly when males are overrepresented in the victim pool of a new trend of crime.

Overshadowing produces limited discussions, limited understanding, and limited preventative measures.

Sextortion research has also typically focused on victims under the age of 18 (Eaton et al., 2022), due to their particular vulnerability to cybersecurity threats, and online exploitation (Jurecic et al., 2016). The average youth is not hyper-secure in their passwords, they often communicate with strangers online, and they are exposed to either sending or receiving pornographic or semi-pornographic content (Jurecic et al., 2016). This makes them vulnerable to sextortion, which is why most research and law enforcement focus on sextortion cases prioritizing minors. Champion & others (2022) note that there is a developing research base for TFSV perpetrated against minors, however, there remains a lack of research regarding TFSV and adult victims. The research gaps surrounding adult male victims contribute to their unjust treatment as victims in TFSV & IBSA. Adults can too be victims, and by acknowledging this, cultural myths can be challenged and a place for research on the subject can be facilitated.

Both a female, and minor-centered lens on sextortion serves as a problem when victims are predominantly males and adults, as noted in financial sextortion (O'Malley, 2023; C3P, 2022). It is important to acknowledge the high victimization levels of females & children in such crimes, however, this lens has limited studies on the role of gender and age in sextortion (Wittes et al., 2016), which poses a problem when unique themes of varying victimization characteristics emerge. A lack of understanding in different victims contributes to a failure in understanding a crime and victim susceptibility, a failure in adequate crime prevention methods, and a failure in assisting victims.

Cyber lifestyles-routine activities theory (CLRAT)

Rooted in both RAT (Cohen & Felson, 1979) and LET (Hindelang et al., 1978, as cited in Dastile, 2004), an integrated paradigm known as Lifestyle-Exposure Routine Activities Theory (LRAT) was introduced. LRAT's significance lies in its examination of victimization from the perspective of opportunity, as well as the lifestyle choices of victims.

RAT proposes that offenders and victims converge contingent in time & space upon three factors, also known as the crime triangle: the presence of a motivated offender (individuals who are capable & willing to commit a crime) a suitable target (an individual that can be readily identified & approached by the motivated offender), and capable guardianship (animate or inanimate barriers that prevent victimization) (Cohen & Felson, 1979; Miro-Llinares, 2014; Vakhitova et al., 2016, as in Nutter, 2021). When all three elements converge in space and time, this creates the opportunity for criminal activity. The opportunity for criminal opportunity is built by LET, which posits that an individual's certain behaviours & lifestyles increase their exposure to motivated offenders (Dastile, 2004); this is known as proximity to motivated offenders, which inherently increases the likelihood of victimization, with the influence of the crime triangle proposed by RAT. In their integration of the two theories, Cohen & colleagues (1981) established four concepts related to the risk of victimization: exposure to motivated offenders, proximity to motivated offenders, target attractiveness to motivated offenders, and capable guardianship.

Throughout the years, LRAT & its main concepts have been translated into cyber-crimes by researchers in only a handful of known studies (Reyns et al., 2011; Holt & Bossler, 2009; Vakhitova et al., 2019; Guerra & Ingram, 2022; Nutter, 2021; Vakhitova et al., 2019).

There is strong support for the application of LRAT in cyber-crimes, however, some researchers have argued against it. Yar (2005) noted differences between virtual & terrestrial environments and the disorganization of time and space in online environments. Yar's (2005) argument against the application of LRAT to virtual environments, suggests that the victim & offender do not converge contingent in time & space in online environments. Due to physical restrictions and distance, there is a divergence in time & space between the victim and the motivated offender. This argument suggests that a suitable target & the motivated offender would not intersect in time & space as they may be from different locations and/or engaging during different time zones.

Eck & Clarke (2003) counter this argument in their study, by modifying RAT's crime triangle, in order to support its applicability to crimes that occur without the physical convergence of a motivated offender & suitable target. The word "place" was replaced with "network" in the crime triangle (Eck & Clarke, 2003). The advancement of the crime triangle in RAT to include "network", acknowledges Yar's (2005) arguments by allowing LRAT's elements to meet without the convergence of offender & target in a physical time and space.

Reyns and colleagues (2011) employed LRAT as a framework in their study of 974 college students, in order to empirically examine victimization in a specific form of cybercrime: cyberstalking. Their study added the word "Cyber" to LRAT and produced CLRAT. Their research addressed the inconsistencies pointed out by Yar (2005) and revised the conceptualization of LRAT into one that considers the divergence in time in space. Reyns & others (2011) expanded the theoretical framework of LRAT and created CLRAT. CLRAT is immensely understudied, and the revised term is rarely used in research exploring cyber victimization. Rather, the theoretical frameworks for RAT are generally incorporated, particularly when a cybercrime is linked to the pandemic’s influence. This is because lockdowns influenced a surge of motivated offenders in cyberspace, “an abundance of suitable targets for predation on proprietary data, personal information, purchasing services and online transactions" (Govender et al., 2021, p. 5), and minimal guardianship as a result of social distancing & the privacy of devices. The crime triangle was prevalent in lockdown times, which explains the primary incorporation of RAT in examining cyber-crimes during the pandemic.

The premise of CLRAT is that individuals who have greater exposure to motivated offenders, greater proximity to motivated offenders, and greater target attractiveness, are hypothesized to be more at risk of victimization; guardianship is the safeguard that disrupts victimization in the face of criminal opportunity (Vakhitova et al., 2019; Reyns et al., 2011; Holt & Bossler, 2009). One criticism against Yar’s (2005) arguments is the theory may be applied too generally to cybercrime, which is why CLRAT is posited to be successful in application when specific cybercrimes are examined (Holt & Bossler, 2009). Therefore, the present study on the specific cybercrime of financial sextortion & its victimization of young males advances research on Reyns & others’ (2011) CLRAT, and its key concepts.

Exposure & Proximity to Motivated Offenders

Exposure refers to the visibility and accessibility of an individual to a motivated offender, whereas proximity is being virtually present & spatially near the domains of influence to potential victimization (Vakhitova et al., 2019). Although exposure and proximity are different concepts, some studies have shared common measures while examining them separately (Reyns et al., 2011; Vakhitova et al., 2019; Holt & Bossler, 2009; Griffith et al., 2023). Due to their similarities in measure, both exposure & proximity are integrated in this study for the examination of victimization.

Exposure and proximity to motivated offenders has typically focused on the behaviour and lifestyles that would potentially expose a suitable target to a motivated offender. Existing literature notes this to be influenced by factors such as internet access, time spent online, activity level of social networking sites, and use of interactive applications (Reyns et al., 2011; Vakhitova et al., 2019; Holt & Bossler, 2009, Holt & Bossler, 2012; Marttila et al., 2021).

Variables of exposure and proximity that place young males susceptible to victimization can be measured not just by their general exposure in cyberspace, but rather, with this population's higher likelihood to engage in a *specific* context of exposure. This is what places young males in closer proximity to a motivated offender. The study by Reyns & colleagues (2011) explored cyberstalking victimization with CLRAT. Their measurements involved the number of photos the respondent posted, the number of daily social network updates respondents performed, the number of social networking accounts they ran, and the use of instant messaging by the respondent (Reyns et al., 2011). Their key finding showed these measurements to have the weakest relationship with victimization (Reyns et al., 2011). This suggests that measuring general online exposure to others through the internt and spending increased time online does not generally mean an individual is in close proximity to a motivated offender, with an increased risk of victimization. Similar to their study, Vakhitova & others (2019) support that a mass presence on social media, or high levels of online self-promotion also do not contribute to a high risk of victimization, as that is just general exposure. Rather it is about high levels of self-promotion or social interaction within a specific context that serves as a better predictor of victimization. Exposure in a "specific context" refers to the number of hours an individual spends in interactive digital settings and engages in risky online behaviors. Interactive digital settings involve discussion forums, online dating sites, instant messaging, and multi-player gaming, (Holt &

Bossler, 2009; Bossler et al., 2012; Reyns et al., 2011; Vakhitova et al., 2019; Griffith et al., 2023). Risky online behaviours that increase proximity to motivated offenders are sexting (Holt & Bossler, 2009; Bossler et al., 2012; Vakhitova et al., 2019), problematic self-disclosure, and allowing strangers into one's social network (Marttila et al., 2021).

Through increased exposure to certain interactive digital settings, young males can come into virtual proximity to motivated offenders (Holt & Bossler, 2009; Bossler et al., 2012; Reyns et al., 2011; Vakhitova et al., 2019; Griffith et al., 2023). Popular interactive settings used among young males are Reddit, Twitch, and other multiplayer game streaming services, such as Xbox, PlayStation Plus, and Nintendo Switch (Vogels et al., 2022). Pew Research Center suggests that boys are substantially more likely to have access to gaming consoles than girls, as this is a major venue for the creation and maintenance of male friendships (Lenhart, 2015). On gaming consoles, males not only engage at a higher frequency than females, but they are significantly more likely to interact with strangers and make new friends (Lenhart, 2015). Participating in forums, apps with instant chats, and/or video streaming services reflects proximity to motivated offenders (Reyns et al., 2011). This was supported in Vakhitova & researchers' (2019) study, as proximity was conceptualized as being virtually present in the domains of influence of potential cyber victimization. By measuring proximity through respondents' participation in online forums and multiplayer gaming, the researchers state that those less likely to be victimized have below average participation in online gaming and chat forums (Vakhitova et al., 2019).

Financial sextortionists not only meet victims on gaming consoles, rather, police have also noted an alarming rise in sextortion in online dating environments (Fong, 2022). A study by Griffith & others (2023) found that online dating was the most likely way for a young person to be exposed to a motivated offender in four different harmful behaviours: hacking, having obscenity shared, bullying, and stalking. On online dating apps, young people are typically scammed through a technique known as catfishing, which is a deceptive activity involving the creation of a fake online profile for deceptive purposes (Harris, 2013, as cited in Smith et al., 2017). Males are more susceptible to victimization this way because they are more likely than women to try online dating, particularly when they are between the ages of 18-29 (Vogels et al., 2023). Pew Research Center notes that about half of users who have used online dating sites and apps come across such scams, and men under 50 are particularly more likely to endure this experience (Vogels et al., 2023).

The second specific type of exposure that increases young males' proximity to motivated offenders are risky online behaviours, such as sexting (Holt & Bossler, 2009; Bossler et al., 2012; Vakhitova et al., 2019). Sexting refers to the sending and receiving of texts, photos, or images that are of a sexual nature. It's a behaviour performed by people to explore and express their sexuality (Klettke et al., 2014; Davidson, 2014). An extensive study about gender & perspectives of sexting by Davidson (2014) reports that both males and females approach sexting differently. For instance, girls view romantic relationships as paramount to their sexting motives, while also noting its potential to destroy their social lives in personal, emotional, and social consequences (Davidson, 2014). Meanwhile, sexting is viewed by a majority of males as connected to peer social relations, and the exercise of power among peers. Boys in the study noted pressures to belong and achieve social status through sexting practices. Davidson (2014) describes how boys believe they are less vulnerable to the consequences of sexting than girls because they care less about their explicit content being exposed. Boys typically do not view the pressure to sext as a threat, but rather as a request (Davidson, 2014). This is contributed to how similar labels of shame in having nudes distributed are not applied to males. Gendered double standards convey shame, humiliation, and social consequences for females who engage in such risky behaviours, with derogatory labels such as “slut” or “whore.” However, if a male’s nudes are distributed, many feel that they are more likely to receive encouragement or praise from their peers (Davidson, 2014).

The specific context of cyber use that young males engage in, makes them susceptible to victimization in financial sextortion. High exposure levels in interactive digital settings, and engagement in risky online behaviours, increase the likelihood of being in closer proximity to motivated offenders. High levels of engagement in such activities among young males seems to be influenced by male culture, and society’s gender double standards, all of which can explain why they are overrepresented as victims in financial sextortion.

Target Attractiveness to Motivated Offenders

A motivated offender’s desirability of a particular person in cyberspace is what is known as target attractiveness. This speaks to the material or symbolic desirability of persons or property targets to potential offenders (Cohen et al., 1981). Studies on cyber victimization have typically focused target attractiveness on how a potential victim is perceived online (Reyns et al., 2011; Rathod et al., 2021; Vakhitova et al., 2019), which is often attributed to their self-disclosure, and whom they self-disclose to. Another measure of a suitable target has been measured among users who visit explicit websites (Griffith et al., 2023), and engage in risky online behaviours (Holt & Bossler, 2009; Bossler et al., 2012; Reyns et al., 2011) such as sexting.

Self-disclosure is an important aspect of victimization as it is a building block for how vulnerable the motivated offender views the potential victim to be. A suitable target will have symbolic value to the offender, while at the same time being perceived as vulnerable to not actively resisting chances at victimization (Vakhitova et al., 2019). General self-disclosure is not a predictor for victimization, rather it is *who* the victim discloses to. Common victim narrative findings from the CP3 report (2022) describe how victims accepted friend requests from strangers. Victims noted being less cautious about these strangers when they had mutual followers/social media friends, and appearance of high engagement, such as a high Snapchat score. Engaging with strangers online may seem harmless, however, those who allow strangers into their online circles are suitable targets in the eyes of a motivated offender (Rathod et al., 2021). This finding can be traced back to how young people engage in social media. For instance, Pew Research Center discovered that roughly half of young people post about personal information, such as their accomplishments, or their family, while others post related to their feelings, dating life, or personal problems (Anderson & Jiang, 2018). There is a vulnerability in self-disclosure, and a motivated offender will look for personal details and images of the potential victim and/or their family & friends in order to legitimize their threats (CP3, 2022; Rathod et al., 2021).

Reyns & colleagues (2011) measured target attractiveness to cyber-victimization through what respondents had disclosed online. This included full name, relationship status, gender, sexual orientation, instant messenger ID, email address, addresses for other social networking blogs/sites, interests and or activities, photos of themselves, and videos of themselves. Bossler & others (2012) also support that those who post personal information online are at greater risk of experiencing online harassment, as this gives prospective offenders information about their target, which can be used in extortion. Some researchers suggest that being single, and/or female holds a higher likelihood for victimization, risk for unwanted contact, harassment victimization, and risk for sexual advances (Reyns et al., 2011). This finding varies from Rathod & others

(2021) who posit that a suitable target for financial sextortion would be a young male. Rathod & colleagues (2021) lay out a primary selection process of a suitable target for a sextortionist: a suitable target will have a high friends number on social media, most of their family &/or friends are also active on social media, and personal details such as school or employment are visible online, and they are well known socially or well respected.

In financial sextortion, a suitable target would be a young male who self-discloses to strangers or allows strangers to inhabit their cyber social circles. When significant details of an individual are available to a motivated offender, they become a suitable target, as this presents an opportunity for the offender to weaponize this information against them.

Guardianship

Guardianship refers to the ability of people or objects to prevent the victimization of a potential target. The presence of a guardian can prevent crime, while its absence increases the likelihood of crime occurring (Felson 1995). In cyberspace, the idea of a "guardian" has often been challenged. For instance, Yar's (2005) assessment of RAT and its applicability to cybercrimes, raised a critical question: are there capable guardians in cyberspace? This was in response to the crime triangle emphasized in RAT, composed of a motivated offender, a suitable target, and the absence of a capable guardian (Cohen & Felson, 1979). Some studies have limited guardianship to a human presence (Hollis et al., 2013), while others have embraced guardianship in various forms such as software filtering, network administrators, firewalls, peer or family intervention, and privacy settings (Vakhitova et al., 2019; Holt & Bossler, 2009; Reyns et al., 2011; Griffith et al., 2023). Guardianship can be measured in three forms, such as physical guardianship, social guardianship, and personal guardianship (Bossler et al., 2012).

The presence of a physical guardian in an online environment protects and impedes the victimization of a potential target. Physical guardianship can be maintained through computer & technology-based protective software, such as privacy settings, profile tracker apps (Bossler et al., 2012), and stronger security reporting functions by platform operators. Bossler & colleagues' (2012) study measured physical guardianship in the online harassment experiences among middle & high school students, by examining the presence of protective software that blocks or filters programs. Utilizing filtering software is a common technique implemented by parents & guardians to protect young suitable targets. Filtering software, such as parental locks help reduce the risk of a child viewing or engaging in inappropriate online content, as it lets guardians monitor internet activity, and the use of age-appropriate settings of devices (Panda Security, 2021). This type of physical guardianship is effective in reducing the odds of victimization among children, however, for adults, this is not always effective. The study by Reyns & others (2011) measured physical guardianship among adults, and they suggest that the use of an online profile tracker is a viable mitigating factor "designed to monitor social network activity so that the user can keep an eye on who is viewing his or her personal information and take preventive measures if troubling patterns develop" (p. 1162). A crucial aspect of this profile tracker variable is that in their study, those using these trackers experienced increased odds of victimization for unwanted cyber contact. A possible explanation the researchers provided for this effect, is that those who experienced problems decided to adopt profile trackers to keep themselves safe in the future (Reyns et al., 2011). For users of digital networking sites, physical guardianship can also exist in platform reporting functions. According to the CP3 report (2022), victims pointed to "platform reporting functions that failed to provide them with options to accurately describe their situation, and a lack of meaningful action being taken by platform operators" (p.4). Platform reporting functions are primarily relevant to adult victims and serve as a significant aspect of their physical guardianship. That said, when platform reporting functions fail to recognize the characteristics of financial sextortion, this lowers the presence of capable guardianship and fails victims in preventative & reactive measures.

The second type of guardianship, known as social guardianship, refers to "the availability of others who may prevent personal crimes by their mere presence, or by offering assistance to ward off an attack" (Spano & Nagy, 2005, p. 418, as cited in Bossler et al., 2012, p. 504). Social guardianship is about intervention, and studies on online victimization have measured this in various ways. For example, Bossler & others (2012) assessed social guardianship by examining the location of the computer during the course of online victimization, as well as how many of the respondents' friends are involved in peer computer deviance. The variable of computer deviance, also referred to as peer deviance, was similarly examined by Reyns & colleagues (2011). They noted an increase in victimization among respondents who believed that their online peers might harass, threaten, or stalk them using the information that they have posted online. This finding is also supported by Holt & Bossler (2009), who examined the role of social guardianship via peer involvement in problematic social media use, and how it influenced online harassment. Their findings suggest that having friends involved in problematic social media use increased the odds of being harassed, as this minimized the number of capable guardians who could assist a potential victim. Digital users who allow strangers into their online communities are more likely to experience a lack of interference, unwanted contact, and harassment, as this portrays a lack of capable guardianship. When males have a higher prevalence of engaging with strangers, such as on gaming consoles (Lenhart, 2015, this indicates low levels of social guardianship, explaining why they are susceptible to victimization.

The final measure of guardianship is personal guardianship, which is a mitigating factor based on a suitable target's own guardianship. This falls under the awareness of guardianship opportunities, often measured in cyberspace by computer skill level, and sharing of personal information (Bossler et al., 2012). Computer skills can also relate to skills of safe cyber use, such as reviewing privacy settings, being aware of social engineering tactics, and reporting suspicious incidents to platforms. Bossler & researchers (2012) examine risky information sharing as a variable of personal guardianship; they examined whether participants communicated with strangers while online, and whether they posted or sent personal information for others they might know only from online to see. According to the C3P report (2022), most victims reported that they lowered their personal guardianship towards potential offenders by allowing them into their online circles after noticing legitimate indicators of true identities, such as high follower numbers or mutual friends. When victims did not lower their personal guardianship towards motivated offenders, some were also approached due to weaker privacy settings on their social media profiles.

Guardianship plays an important role in the hindrance of victimization in financial sextortion. When young males lower their personal guardianship through weak privacy settings or endanger their social guardianship by engaging with & befriending strangers online, they are susceptible to victimization. Alas, once victims do attempt to regain control of the situation, they are failed by platform reporting functions that prevent them from accurately voicing their experiences.

Modus Operandi

Modus Operandi, a Latin phrase that means “method of operating” in English, refers to a pattern of learned behaviours that are adopted by an offender to secure a victim’s compliance in order to commit their crime. An MO is dynamic & malleable and is composed of behaviours exhibited by an offender before, during, and after the crime is committed (Leclerc et al., 2009). In studying the manner in which a crime is committed, MO is a crucial element of understanding a criminal phenomenon. This part of the literature review covers how a classic case of financial sextortion would occur, further dissecting the MO by focusing on common behaviours displayed during the possession, and the extortion stage of the crime.

A Conventional Case of Financial Sextortion

Europol’s (2017) report on online sexual coercion and extortion proposed an offender profile that characterizes what kind of motivated offenders engage in this crime. According to their profile, a financial sextortionist could be male or female, however, they are most often a member of an organized criminal group (Europol, 2017). This point is also supported by other organizations as they note the perpetrators to be operating from countries such as Nigeria, Cote D’Ivoire and the Philippines (C3P, 2022; RCMP, 2023; U.S Immigration and Customs Enforcement [ICE], 2023; ALERT, 2022). These motivated offenders act on both an international and domestic level as they search for victims, however, they are more likely to approach individuals who are from countries that are linked by the same language, as that of the offender (Europol, 2017). This suggests that a sextortionist is versed in a wide range of languages, particularly English (Europol, 2017). The victim & the financial sextortionist are strangers who encounter one another in cyberspace (Europol, 2017; Ibrahim, 2022), and the primary motive of the offender is to obtain money.

A study by Rathod & other researchers (2021) analyzed an incident between one of the researchers and a sextortionist. The study noted how the offenders followed the almost same MO in the incident that has been present in the majority of financial sextortion cases victimizing young men (C3P, 2022). According to the researchers (Rathod et al., 2021), a conventional plan by a motivated offender in financial sextortion, begins with the creation of a fake social media account. By acquiring a profile picture of a young girl, the motivated offender searches for random users on a platform, in order to identify suitable targets. After selecting a suitable target, the sextortionist sends a friend request, which then leads to instant contact via messaging. The communication between the motivated offender & suitable target often shifts to another platform that allows the sharing of images or has video calling features, such as Snapchat or WhatsApp. This conversation will quickly escalate into a sexual context, in which the motivated offender will request for a video chat, or for sexually explicit images from the target. During the sexual encounter, a pre-recorded pornographic video or modified explicit content is shown to the victim, as a way to invoke reciprocity. During this encounter, the victim's sexual behaviours are secretly recorded, as this is proof of their sexual conduct. The conversation will instantly shift into extortion, in which the offender demands a sum of significant money, or else the explicit material will be distributed. The sextortionist will provide the victim with financial transfer details, and during extortion, they attempt to evoke strong emotions in the victims to have their demands met.

Possession

The possession stage of financial sextortion refers to how the offender comes to possess obscene images or videos of the victim. In this stage, sextortionists use a variety of tactics laced with manipulation to obtain explicit content from their victims. When victims are children, the most frequent method of obtaining explicit material is done through grooming. Grooming is a process in which a sexually motivated offender desensitizes the victim to make them less likely to reject or report the abusive behaviour; this is done by developing sexual conversations, building trust, and promoting silence (Bull & Page, 2021; O'Malley & Holt, 2022). By establishing a groomed relationship, created on the basis of a power imbalance, the offender gradually increases the confidence of the victim and persuades them to perform obscene acts (Acar, 2016). Although adults can also be groomed (Bull & Page, 2021), grooming is typically noticed among minor-focused offenders who are sexually attracted to children (O'Malley & Holt, 2022). Grooming is not a primary process used by financial sextortionists, as grooming takes more time between an offender and a victim since trust & a bond are established. Meanwhile, financially motivated sextortion progresses rapidly in a time-sensitive manner (O'Malley & Holt, 2022) since the main motive of the offender is money.

In financial sextortion, impersonation is a primary behaviour perpetrated by offenders, where they deceive victims into believing that they are communicating online with a similar-aged peer, particularly a young girl. This is performed in order to seduce the victim and manufacture trust, eventually creating a sense of reciprocity within image-sharing (O'Malley & Holt, 2022). Sextortionists trick the victim into believing that the stranger & the victim share something in common, which could be the same school, city, or mutual friends; this is performed in order to legitimize their fabricated identity and to create familiarity.

Another noted behaviour among financial sextortionists is the utilization of a secondary social networking platform. According to the C3P report (2022), when posing as a female, offenders first contact the victim on Instagram, and soon transfer the conversation to snapchat, where they entice the victim to send explicit images. Snapchat is a highly referenced secondary app in the victim narratives (C3P, 2022), and offenders may be transferring conversations to this app due to the sense of security the platform provides for deviant behaviour. For instance, Snapchat allows users to send and receive photos & videos, allows messages to be ultimately deleted from the servers & the engaged accounts (Poltash, 2013), and a location-sharing feature known as Snap Maps, which allows users to not only view each other's whereabouts, but it's “our Story” feature allows them to post stories that can be seen by anyone in the world (Harris, 2018). Snapchat is an oasis for sextortionists to find, target, and exploit victims. In their primary selection of young males as targets, financial sextortionists may also utilize Snapchat as a core environment for possession, due to how the app is used among young males. For instance, a study by Moran & colleagues (2018) found that women do not use Snapchat to continuously send naked images or videos, rather men are more likely to use the app to gain sexual access, hookups, and to continue sending naked images.

During the image-sharing stage that often takes place in the secondary app, the offender tries to legitimize their identity. As common victim narratives note, the offenders “had a consistent face from the snaps” (C3P, 2022, p. 15). These types of tactics legitimize the identity of the offender and create a sense of trust in the victim. A sexual element is then introduced to the conversation, either through flirtatious messages, or by sending sexual images. A victim from the Reddit page said, “the scammer sent some nude images, and I stupidly sent some back” (C3P, 2022, p. 15). This is a strategy performed by the offender in order to invoke reciprocity within image sharing. However, what the victim sees is fabricated content, such as pre-recorded sexual images or videos, that are shown consistently in order to trick the victim into sharing their explicit content.

Extortion

The extortion stage of financial sextortion begins as soon as the offender comes to possess the sexual images or videos from the victim. The MOs in extortion are composed of methods of threat or intimidation that the sextortionist uses to gain financial benefit. Financial sextortionists thrive off the heightened emotions of their victims, as this is why threats are made in a time-sensitive manner. The entire victimization process can occur within a matter of minutes, or hours. This is conducted by intimidating the victim, which is carried out by sharing screenshots of their location, and means of contacting their family, friends, or school (C3P, 2022; Rathod et al., 2021).

Daniel Lints, a 17-year-old male from rural Manitoba was contacted by a financial sextortionist in February 2022. After being coerced into sending his explicit images, Daniel faced extortion within minutes. After intimidation, he complied with the offender's demands, and within three hours, Daniel took his own life (Malone, 2022).

Several news medias have captured the stories of numerous other victims similar to Daniel, who were strongly impacted by the intimidating behaviours of the sextortionist (Campbell & Kravarik, 2022; Spocchia, 2022; Larson & Nesbitt, 2022; Reily, 2023; Andaloro, 2023). Suicide is a pattern noted among victims of TFSV (Champion et al., 2021, as cited in O'Malley, 2023). This is attributed to the emotional unrest that is produced by the manipulative tactics employed by sextortionists. For example, feelings of fear, helplessness, hopelessness, shame, self-blame, humiliation, and general distress are commonly experienced by victims (Nilsson, 2019). The intimidation tactics that are used against the victim produce these emotions on the basis of primary victimization (victimization by the offender), and secondary victimization. Secondary victimization includes the aftermath of what could occur as a result of primary victimization. For instance, many victims of financial sextortion who have their explicit images distributed may experience cyberbullying, strained relationships, and substantial disruptions in their lives (O’Malley, 2023).

Male victimization to a crime that is primarily viewed as a female-centered offence, comes with the confusion of understanding one’s own victimization, and how others may react to it. As a way to avoid such repercussions, financial sextortion goes significantly underreported, and in unfortunate circumstances, the victims resort to suicide. Such stressful emotions that are created as a result of intimidation, impact males and places them susceptible to victimization.

Conclusion and Recommendations

Technological advancements have enhanced social connectedness for both romantic and sexual encounters. Covid-19 was a key contributor to such advancements, as a time of lockdowns had technology being utilized more than ever in the form of online school and remote working. However, as cyber use increased, so did its risks.

The present study explores the evolving phenomenon of financial sextortion and its primary victimization of young males. By examining victimization through CLRAT & its key concepts, and offending behaviours through an examination of MO, the findings answer how young males are susceptible to victimization, and how the crime unfolds.

The data regarding victimization highlighted the specific cyberspace behaviours performed by young males that render them susceptible to victimization. High levels of exposure among young males in interactive digital settings and risky online behaviours, increases proximity to a motivated offender. The high young male prevalence of interacting on gaming consoles with strangers, sexting by the influence of gendered social norms, and utilizing apps for sexual purposes, makes them a suitable target in the eyes of a financial sextortionist.

The results also highlight how guardianship is weakened when young males interact online with strangers, allow strangers to access their cyber social circles under false identities, and how victims are ultimately failed by weak platform reporting functions.

An examination of MO presents the manipulative tactics of the offenders used in both the possession and extortion stages of the crime. Offenders employ behaviours such as impersonation, the transference of the crime to a secondary platform, the portrayal of fabricated explicit content, and the use of intimidation threats in their general MO.

By enhancing the discussion of male victimization in IBSA & TFSV, this study contributed to the misconceptions surrounding sextortion and the under-protection of non-conventional victims, such as adult males. The inadequacy of legislation, investigative barriers, and reporting functions available to victims have created challenges to countering sextortion.

The first recommendation from the findings of this study is for lawmakers in Canada & across the world to adopt a federal statute that addresses the specific conducts of the unique ways sextortion can manifest itself. In most countries, law enforcement continues to rely on a patchwork of laws that insufficiently cover the diverse nature of the crime (France, 2022). When political discussion takes place for the implementation of specific legal frameworks surrounding sextortion, this could help fill in legal loopholes, and raise awareness for the public, as well as offer clarity for law enforcement (France, 2022). Potential statutes should address the various themes & elements of sextortion that could occur, even when explicit images are not distributed. Potential laws should avoid terminology of a gender-based lens and offer protection to adult victims without the mere safeguards of child pornography laws. Potential statutes should treat the age of the victim as an aggravating factor, instead of as a core element of the offense (Wittes et al., 2016). Due to the crime's transnational nature, such a statute should be implemented into federal law. By legally defining & implementing sextortion as a federal criminal offence, will offer clarity for law enforcement, and recognition for various sextortion victims & their families for the psychological & emotional harm they have endured (Canadian Press, 2022), even if their pictures were not non-consensually shared. A common argument against laws that are narrowly focused is that generalized laws allow police more freedom when it comes to charges. However, there are benefits to explicitly proscribing sextortion in the law. The first step of implementing a legal definition of sextortion is a step in the direction of acknowledging this as a serious crime. When certain behaviours are legally forbidden, it not only acts as a deterrence, but it also assists victims recognize when they are victimized.

The second recommendation is a call for financial sextortion offences to be handled by federal authorities. Financial sextortion occurs in a transnational & organized way which is beyond the scope of local agencies alone. Sextortion occurs in a domain that is boundaryless, often requiring complex inter-jurisdictional designs and technical forensics (Wittes et al., 2016). Federal authorities are better positioned for such interstate & international investigations than local authorities, as they also have stronger laws & penalties. Financial sextortion should be handled among entities such as the Canadian Security Intelligence Service (CSIS), Royal Canadian Mountain Police (RCMP), and the Canadian Border Services Agency (CBSA).

The third recommendation falls under guardianship & safe cyber use. Many victims from the C3P report pointed out the inadequate "platform reporting functions that failed to provide them with options to accurately describe their situation and a lack of meaningful action being taken by platform operators" (C3P, 2022, p. 4). Social media platforms should provide reporting options specific to blackmail and extortion that are responsive and capture the seriousness of users being aggressively and actively targeted. Several victims encounter reporting menus that fail to capture their victimization or the urgency of the matter. Even once an offender's account was reported, some accounts often remained active, allowing access to the victim; in other scenarios, offenders were able to access victims through separate accounts when the initial account was blocked, deleted, or removed by the platform operators (C3P, 2022).

The final recommendation calls for a primary research project that is funded and conducted in order to understand the first-hand experiences of victims and their needs. The main limitation of the present study is the use of secondary data. Although the collection of secondary data is less time consuming, and useful in conducting exploratory research, it was not as comprehensive as what firsthand exposure could provide. A primary research project is better suited to meet for more reliable victim narratives, control over data quality, and for avoiding biases in the sources gathered.

References

Acar, K. V. (2016). Sexual extortion of children in cyberspace. *International Journal of Cyber Criminology*, *10*(2), 973–5089. https://doi.orgg/10.5281/zenodo.163398/

Alberta Law Enforcement Response Teams. (2022). *Sextortion is real and it's happening in Alberta more than ever before. https://alert-ab.ca/public-knowledge/sextortion/*

Andaloro, A. (2023, January 5). Former homecoming king and athlete, 17, died by suicide after sextortion plot. *Little Things.* https://littlethings.com/lifestyle/michigan-teen-suicide-sextortion

Anderson, M., & Jiang, J. (2018). *Teens and their experiences on social media.* Pew Research Center. https://www.pewresearch.org/internet/2018/11/28/teens-and-their-experiences-on-social-media/

Anderson, J., Raine, L., & Vogels, E.A. (2021). *Experts say the new normal in 2025 will be far more tech-driven, presenting more big challenges.* Pew Research Center. https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges/

Bilodeau, H., Kehler, A., & Minnema, N. (2021). *Internet use and COVID-19: How the pandemic increased the amount of time Canadians spend online*. (Catalogue No. 45-28-0001). Statistics Canada. https://www150.statcan.gc.ca/n1/en/pub/45-28-0001/2021001/article/00027-eng.pdf?st=h9jXyWgY

Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting online harassment victimization among a juvenile population. *Youth & Society, 44*(4), 500–523. https://doi.org/10.1177/0044118X11407525

Bull, A., & Page, T. (2021). Students' accounts of grooming and boundary-blurring behaviours by academic staff in UK higher education. *Gender and Education, 33*(8), 1057–1072. https://doi.org/10.1080/09540253.2021.1884199

Campbell, J., & Kravarik, J. (2022, May 21). A 17-year-old boy died by suicide hours after being scammed: The FBI says its part of a troubling increase in sextortion cases. *CTV News. https://www.ctvnews.ca/world/a-17-year-old-boy-died-by-suicide-hours-after-being-scammed-the-fbi-says-it-s-part-of-a-troubling-increase-in-sextortion-cases-1.5913698*

Canadian Centre for Child Protection. (2022). *An analysis of financial sextortion victim posts on r/sextortion. https://protectchildren.ca/en/resources-research/an-analysis-of-financial-sextortion-victim-posts-published-on-sextortion/*

Canadian Press. (2022). *Amanda Todd sextortion case sets precedent, but more needs to be done: experts.* PentictonNow. https://www.pentictonnow.com/watercooler/news/news/Provincial/Amanda_Todd_sextortion_case_sets_precedent_but_more_needs_to_be_done_experts/#fs_121090

Champion, A. R., Oswald, F., Khera, D., & Pedersen, C. L. (2022). Examining the gendered impacts of technology-facilitated sexual violence: A mixed methods approach. *Archives of Sexual Behavior, 51*(3), 1607–1624. https://doi.org/10.1007/s10508-021-02226-y

Cohen, L.E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American Sociological Review*, *46*(5), 505–524. https://doi.org/10.2307/2094935

Convention on the Rights of the Child. (1989). Treaty no. 27531. United Nations Treaty Series, 1577, pp. 3-178. Available at: https://treaties.un.org/doc/Treaties/1990/09/19900902%2003-14%20AM/Ch_IV_11p.pdf (Accessed: 24, January 2023).

Criminal Code, RSC 1985, c C-46. https://laws-lois.justice.gc.ca/PDF/C-46.pdf

Dastile, N.P. (2004). Chapter 3: Theoretical perspective (Eds.), *University of Pretoria: Open Repository.* https://repository.up.ac.za/bitstream/handle/2263/22884/03chapter3.pdf?sequence=4&isAllowed=y#:~:text=interpersonal%20contacts%20decrease.-,Hindelang%20et%20al.,not%20available%20as%20potential%20victims.&text=Gender%20also%20plays%20an%20important,individual's%20routine%20activities%20and%20lifestyle

Davidson, J. (2014). Sexting: Gender and teens. *Sense Publishers*

Eaton, A. A., Ramjee, D., & Saunders, J. F. (2022). The relationship between sextortion during COVID-19 and pre-pandemic intimate partner violence: A large study of victimization among diverse U.S men and women. *Victims & Offenders*, *18*(2), 338–355. https://doi.org/10.1080/15564886.2021.2022057

Eck, J & Clarke, R.V. (2003). Classifying common police problems: A routine activity approach. *Crime Prevention Studies*, *16*, 7-39. https://doi.org/www.researchgate.net/publication/303564787_Classifying_commonpolice_problems_A_routine_activity_approach

Europol. (2017). *Online sexual coercion and extortion as a form of crime affecting children: Law enforcement perspective.* https://www.europol.europa.eu/cms/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf

Federal Bureau of Investigation. (2019). *FBI launches sextortion awareness campaign in schools: Youth should be on guard online.* https://www.fbi.gov/news/stories/stop-sextortion-youth-face-risk-online-090319

Felson, M. (1995). *Those who discourage crime*. Rutgers University.https:doi.org/www.researchgate.net/publication/248079176_Those_who_discourage_crime

France, G. (2022). *Criminalising sextortion: Challenges and alternatives.* Transparency International. https://knowledgehub.transparency.org/assets/uploads/kproducts/Criminalising-sextortion_final_10.06.2022.pdf

Franklin, Z. (2014). Justice for revenge porn victims: Legal theories to overcome claims of civil immunity by operators of revenge porn websites. *California*

Law Review, *102*(5), 1303–1335. https://doi.org/www.californialawreview.org/wp-content/uploads/2014/12/05-Franklin.pdf

Fong, G. (2022, November 8). *Sextortion on dating apps hits alarming rates: Here's how to protect yourself*. HypeBae. https://doi.org//hypebae.com/2022/11/what-is-sextortion-scams-safety-dating-app-expert-advice

Govender, I., Watson, B.W.W, & Amra, J. (2021). Global virus lockdown and cybercrime rate trends: A routine activity approach. *Journal of Physics: Conference Series, 1828*, 1-8. https://doi.org/10.1088/1742-6596/1828/1/012107

Griffith, C. E., Tetzlaff-Bemiller, M., & Hunter, L. Y. (2023). Understanding the cyber-victimization of young people: A test of routine activities theory. *Telematics and Informatics Reports.* https://doi.org/10.1016/j.teler.2023.100042

Guerra, C., & Ingram, J.R. (2022). Assessing the relationship between lifestyle routine activities theory and online victimization using panel data. *Deviant Behavior. 43*(1), *44-60.* https://doi.org/10.1080/01639625.2020.1774707

Haslam, C., Cruwys, T., Haslam, S.A., & Jetten, J. (2015). Social connectedness and health. *Encyclopedia of Geropsychology*. https://doi.org/10.1007/978-981-287-080-3_46-2, 46-1.

Harris, K. (2018). T*he dangers of snapmap on snapchat*. Learn Safe. https://learnsafe.com/the-dangers-of-snap-map-on-snapchat/

Henry, N., & Powell, A. (2016). Sexual violence in the digital age: The scope and limits of criminal law. *Social & Legal Studies, 25*(4), 397–418. https://doi.org/10.1177/0964663915624273

Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence & Abuse, 19*(2), 195–208. https://doi.org/10.1177/1524838016650189

Hollis, M. E., Felson, M., & Welsh, B. C. (2013). The capable guardian in routine activities theory: A theoretical and conceptual reappraisal. *Crime Prevention and Community Safety, 15*(1), 65-79. https://doi.org/10.1057/cpcs.2012.14

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1–25. https://doi.org/10.1080/01639620701876577

Ibrahim, D. (2022). *Online child sexual exploitation and abuse in Canada: A statistical profile of police-reported incidents and court charges, 2014 to 2020* (Catalogue No. 85-002-X). Statistics Canada. https://www150.statcan.gc.ca/n1/en/pub/85-002-x/2022001/article/00008-eng.pdf?st=OqSZdAtG

International Association of Women Judges. (2012). *Stopping the abuse of power through sexual exploitation: Naming, shaming and ending sextortion. https://www.unodc.org/res/ji/import/guide/naming_shaming_ending_sextortion/naming_shaming_ending_sextortion.pdf*

INTERPOL. (2022). *Asia: Sextortion ring dismantled by Police.* https://www.interpol.int/en/News-and-Events/News/2022/Asia-Sextortion-ring-dismantled-by-police

Jurecic, Q., Spera, C., Wittes, B., & Poplin, C. (2016). *Sextortion: The problem and solutions.* Brookings Institution. https://www.brookings.edu/blog/techtank/2016/05/11/sextortion-the-problem-and-solutions/

Kajal, K. (2022). *The Sextortion scammers of rural India*. Rest of World. https://restofworld.org/2022/sex-scam-village-india/

Klettke, B., Hallford, D.J., Mellor, D.J. (2014). Sexting prevalence and correlates: A systematic literature review. *Clinical Psychology Review, 34*(1). 44-53 https://doi.org/10.1016/j.cpr.2013.10.007

Korkmazer, B., De Ridder, S., & Van Bauwel, S. (2020). Reporting on young people, sexuality, and social media: a discourse theoretical analysis. *Journal of Youth Studies, 23*(3). 323-339. Routledge. https://doi.org/10.1080/13676261.2019.1603365

Larson, A., & Nesbitt, R. (2022, December 19). San Jose police: Teen boys fell victim to sextortion, 1 killed self. *Kron4.* https://www.kron4.com/news/bay-area/san-jose-police-teen-boys-fell-victim-to-sextortion-1-killed-self/

Leclerc, B., Proulx, J., Lussier, P., & Allaire, J.-F. (2009). Offender victim interaction and crime event outcomes: Modus operandi and victim effects on the risk of intrusive sexual offenses against children. *Criminology, 47*(2), 595–618. https://doi.org/10.1111/j.1745-9125.2009.00151.x

Lenhart, A. (2015). *Chapter 3: Video games are key elements in friendships for many boys*. Pew Research Center. https://doi.org/www.pewresearch.org/internet/2015/08/06/chapter-3-video-games-are-key-elements-in-friendships-for-many-boys/

Luo, & Hancock, J. T. (2020). Self-disclosure and social media: motivations, mechanisms and psychological well-being. *Current Opinion in Psychology*, *31*, 110–115. https://doi.org/10.1016/j.copsyc.2019.08.019

Malone, G.K. (2022, June 19). World lost a good person: Manitoba parents warn of global sextortion targeting teenage boys. *The Canadian Press.* https://www.cbc.ca/news/canada/manitoba/manitoba-sexploitation-suicide-1.6494054

Marttila, E., Koivula, A. & Räsänen, P. (2021). Cybercrime victimization and problematic social media use: Findings from a nationally representative panel study. *American Journal of Criminal Justice, 46*, 862–881. https://doi.org/10.1007/s12103-021-09665-2

Miró-Llinares, F. (2014). Routine activity theory. The Encyclopedia of Theoretical Criminology Online. *Blackwell 0*(0), 1-7. https://doi.org/10.1002/9781118517390/wbetc198

Moreau, G. (2022). Police-reported crime statistics in Canada, 2021. (Catalogue No. 85-002-X. Statistics Canada. https://www150.statcan.gc.ca/n1/en/pub/85-002-x/2022001/article/00013-eng.pdf?st=nMHYBqcP

Moran, J. B., Salerno, K. J., & Wade, T. J. (2018). Snapchat as a new tool for sexual access: Are there sex differences? *Personality and Individual Differences*, *129*, 12–16. https://doi.org/10.1016/j.paid.2018.02.040

National Center for Missing and Exploited Children. (2023). *Sextortion*. https://www.missingkids.org/theissues/sextortion#bythenumbers.

Nabity-Grover, T., Cheung, C. M. K., & Thatcher, J. B. (2020). Inside out and outside in: How the COVID-19 pandemic affects self-disclosure on social media. *International journal of information management*, *55*, 102188. https://doi.org/10.1016/j.ijinfomgt.2020.102188

Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*, *2*(2), 175–220. https://doi.org/10.1037/1089-2680.2.2.175

Nilsson, M. G., Tzani-Pepelasis, C., Ioannou, M., & Lester, D. (2019). Understanding the link between sextortion and suicide. *International Journal of Cyber Criminology, 13*(1), 55–69. https://doi.org/10.5281/zenodo.3402357

Nutter, K.J. (2021) Examining cyberstalking victimization using routine activities and lifestyle routine activities theories: A critical literature review. T*he Mid-Southern Journal of Criminal Justice*, *20(4)*. https://mds.marshall.edu/msjcj/vol20/iss1/4

O'Malley, R. L., & Holt, K. M. (2022). Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime. *Journal of Interpersonal Violence*, *37*(1-2), 258–283. https://doi.org/10.1177/0886260520909186

O'Malley, R. L. (2023). Short-term and long-term impacts of financial sextortion on victim's mental well-being. *Journal of Interpersonal Violence.* https://doi.org/10.1177/08862605231156416

Patchin, J. W., & Hinduja, S. (2020). Sextortion among adolescents: Results from a national survey of U.S. youth. *Sexual Abuse, 32*(1), 30–54. https://doi.org/10.1177/1079063218800469

Panda Security. (2021, April). *How to set parental controls on all your devices.* https://www.pandasecurity.com/en/mediacenter/panda-security/parental-control/

Pollard, S.E., and Kuznar, L. (2022). A world emerging from pandemic: Implications for intelligence and national security. *National Intelligence University*. https://irp.fas.org/eprint/pandemic.pdf

Poltash, N.A. (2013). Snapchat and sexting: A snapshot of baring your bare essentials. *Richmond*

Journal of Law and Technology, 19(1), 10-12. http://jolt.richmond.edu/v19i4/article14.pdf.

Rathod, S., Gaur, M., Parihar, K., Kumar, A., & Jain, D. (2021). Tracing of the blackmailers in sextortion case and tactics to defend it : An experimental cybercrime case study. *International Journal of Scientific Research in Science and Technology*, 135-142. http://doi.org/10.32628/CSEIT217414.

Reclaim Pro Bono. (2022). *Legislation and cases. https://reclaimprobono.org/information/the-law/*

Reiter, B. (2017). Theory and methodology of exploratory social science research. *Government and International Affairs Faculty Publications*. https://digitalcommons.usf.edu/gia_facpub/132

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Reily, R. (2022, February 22). Imagine the panic: A teen was catfished, extorted, and took his own life. Now his father is speaking out. *USA Today.* https://www.usatoday.com/story/news/nation/2023/02/22/mississippi-teen-sextortion-case-dangers/11324554002/

Royal Canadian Mountain Police. (2023). *Online scammers are the ones asking for nude photos and money: Educate yourself to better protect yourself from sextortion.* https://www.rcmp-grc.gc.ca/en/news/2023/online-scammers-are-the-ones-asking-nude-photos-and-money-educate-better-protect#:~:text=Financial%20sextortion%20is%20a%20type,others%20unless%20you%20pay%20them.

Roebuck, B., McGlinchey, D., Hastie, K., Taylor, M., Roebuck, M., Bhele, S., Hudson, E., & Xavier, R.G. (2020). *Male survivors of intimate partner violence in Canada.* Office of the Federal Ombudsman for Victims of Crime. https://www.victimsfirst.gc.ca/res/cor/IPV-IPV/Male%20Survivors%20of%20IPV%20in%20Canada,%202020.pdf

Shaw, N. (2022). Reports of extortion double in a year and make up the biggest issue for helpline. *Wales Online.* https://www.walesonline.co.uk/news/uk-news/reports-sextortion-double-year-make-24010796

Smith, L. R., Smith, K. D., & Blazka, M. (2017). Follow me, what's the harm? considerations of catfishing and utilising fake online personas on social media. *Journal of Legal Aspects of Sport*, *27*(1), 32–45. https://doi.org/10.1123/jlas.2016-0020

Spocchia, G. (2022, May 22). Mother of 17-year-old boy who died by suicide after being targeted by sextortionist online issues warning. *Independent*. https://www.independent.co.uk/news/world/americas/crime/california-teen-suicide-sextortionist-b2084575.html

University of North Dakota. (2023). *Literature review.* https://libguides.und.edu/literature-reviews

U.S. Immigration and Customs Enforcement [ICE]. (2023). Sextortion: It's more common than you think. *Department of Homeland Security.* https://www.ice.gov/features/sextortion

Vakhitova, Z. I., Alston-Knox, C. L., Reynald, D. M., Townsley, M. K., & Webster, J. L. (2019).

Lifestyles and routine activities: Do they enable different types of cyber abuse? *Computers in Human Behavior, 101*, 225–237. https://doi.org/10.1016/j.chb.2019.07.012

Vogels, E.A., & Mcclain, C. (2023). *Key findings about online dating in the U.S.* Pew Research Center. https://www.pewresearch.org/fact-tank/2023/02/02/key-findings-about-online-dating-in-the-u-s/

Vogels, E.A., Gelles-Watnick, R., & Massarat, N. (2022). *Teens, social media, and technology 2022*. Pew Research Center. https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/

Wittes, B., Poplin, C., Jurecic, Q., and Spera, C. (2016). Sextortion: Cybersecurity, teenagers, and remote sexual assault. *Brookings Institution: Center for Technology Innovation.* https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf

Wittes, B., Poplin, C., Jurecic, Q., and Spera, C. (2016). Closing the sextortion sentencing gap: A legislative proposal. *Brookings Institution: Center for Technology Innovation. https://www.brookings.edu/research/closing-the-sextortion-sentencing-gap-a-legislative-proposal/*

Yadav, Y. (2022). *India becoming sextortion capital of the world?* The Times of India. https://timesofindia.indiatimes.com/blogs/voices/india-becoming-sextortion-capital-of-the-world

Yar, M. (2005). The novelty of cybercrime: An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407-427. http://dx.doi.org/10.1177/147737080556056