Victims & Offenders
An International Journal of Evidence-Based Research, Policy, and Practice
Volume 20, Numbers 5-6, 2025
ISSN: 1556-4886
Editor-in-Chief
James M. Byrne
Co-Editor-in-Chief
Donald Hummer
Numbers 5-6
Special Issue: Theoretical Approaches in Victimology Research
Guest Editors: Eileen M. Ahlin and Maria João Lobo Antunes
Routledge
Taylor & Francis Group

Routledge
Taylor & Francis Group

Victims & Offenders

An International Journal of Evidence-based Research, Policy, and Practice

ISSN: 1556-4886 (Print) 1556-4991 (Online) Journal homepage: www.tandfonline.com/journals/uvao20

Explaining Image-Based Sexual Abuse: An Application of Cyber Routine Activity Theory

Albina Laskovtsov & Kaitlin M. Boyle

To cite this article: Albina Laskovtsov & Kaitlin M. Boyle (2025) Explaining Image-Based Sexual Abuse: An Application of Cyber Routine Activity Theory, Victims & Offenders, 20:5-6, 1059-1085, DOI: 10.1080/15564886.2025.2485125

To link to this article: https://doi.org/10.1080/15564886.2025.2485125

Published online: 05 Aug 2025.

VICTIMS & OFFENDERS
2025, VOL. 20, NOS. 5–6, 1059–1085
https://doi.org/10.1080/15564886.2025.2485125

Routledge
Taylor & Francis Group

Explaining Image-Based Sexual Abuse: An Application of Cyber Routine Activity Theory

Albina Laskovtsov[a] and Kaitlin M. Boyle[b]

[a]Department of Social Sciences, Shepherd University, Shepherdstown, West Virginia, USA; [b]Department of Criminology and Criminal Justice, University of South Carolina, Columbia, South Carolina, USA

ABSTRACT
This work focuses on image-based sexual abuse (IBSA), which involves the creation, dissemination, and/or threats to create or disseminate illicit sexual media without one's consent. While much research is produced on cyber victimization in general, there remains a dearth of literature on theoretical explanation of IBSA victimization. This study aims to theoretically assess the applicability of a traditionally physical theory of crime, routine activity theory, to explain a digital form of interpersonal abuse: IBSA. This study relies on survey data of 506 18-to -24 year-old women in the United States to examine their experiences of six different types of IBSA: (1) creation of sexualized media, (2) dissemination of sexualized media, (3) being threatened with the creation or dissemination of sexualized media, (4) creation of media depicting unwanted sexual experiences, (5) dissemination of media depicting unwanted sexual experiences, and (6) sextortion. The current study asks what protective and risk factors are associated with the likelihood of experiencing IBSA? In analyzing a series of logistic regressions, the results indicate that spending time online, sexting, and proximity to motivated offenders in the form of association with deviant peers is correlated with IBSA victimization. These risk factors can assist in intervention and prevention responses to this form of abuse; however, these results indicate the feasibility of integration of a feminist lens through which to assess IBSA victimization.

KEYWORDS
Image-based sexual abuse; routine activity theory; victimological theory; risk factors

Introduction

In recent years, cybervictimization scholarship has expanded and grown through empirical research and theoretical application; however, specific attention to image-based sexual abuse (IBSA), particularly as it relates to victimological theory, is lacking. IBSA involves three behaviors: creating, disseminating, and/or threatening to create or disseminate illicit sexual media without one's consent or permission (Henry & Flynn, 2019; Henry et al., 2021; McGlynn & Rackley, 2017; Powell & Henry, 2017). These media include images and videos depicting nude or seminude individuals that are often displayed in a sexualized manner, in some cases without the knowledge of the victim. It has been estimated that as many as one in eight Americans have experienced the non-consensual dissemination of sexualized, explicit media (Eaton et al., 2017), and studies utilizing purposive and convenience

CONTACT Albina Laskovtsov alaskovt@shepherd.edu Department of Social Sciences, Shepherd University, PO Box 5000, Shepherdstown, WV 25443, USA

sampling, particularly on college campuses, find prevalence rates ranging from 10% (Branch et al., 2017) to 84% (Snaychuk & O'Neill, 2020).

IBSA occurs in a variety of contexts. Most commonly, a sexual intimate image or video is taken consensually and shared with a consenting partner or acquaintance, who then maliciously posts or distributes it to others without consent; alternatively that consensual image may be obtained through more nefarious means, such as cyberhacking and data breaching (Franks, 2017; Krieger, 2017). IBSA includes acts of voyeurism like taking pictures or videos up someone's skirt or dress or down their shirt, "in circumstances whereby a person would have a reasonable expectation of privacy" (Fisico & Harkins, 2021, p. 59). Other forms of IBSA are found in the creation of deepfakes, which are fictitious photo-shopped images of a person's likeness onto pornographic media, often through artificial intelligence (A.I.) programs and tools (Eaton & McGlynn, 2020; Flynn et al., 2021); sexual extortion, in which an individual's private and intimate images and videos are used as blackmail to coerce more images or sexual acts (Cross et al., 2022; Eaton & McGlynn, 2020); and the use of digital platforms to plan a physical sexual assault (Fisico & Harkins, 2021; Powell & Henry, 2019).

Though it is difficult to effectively capture IBSA victimization prevalence rates across demographic groups since studies tend to rely on diverse and heterogenous samples without a reliance on a standard definition of IBSA (Paradiso et al., 2024), scholars argue that IBSA is a growing and evolving concern that directly impacts people's lives in detrimental and complex ways (Henry & Flynn, 2019; Henry et al., 2021; McGlynn & Rackley, 2017; McGlynn et al., 2017; Powell & Henry, 2017). Researchers have found evidence of relationships between IBSA victimization and diminished mental health (Bates, 2017; Champion et al., 2022; Huber, 2023; Ruvalcaba & Eaton, 2020), physical health (Huber, 2023; Ruvalcaba & Eaton, 2020), social well-being (Campbell et al., 2020), academic and work success (Bates, 2017), and the development of substance use disorders (Champion et al., 2022). The current study contributes to the ongoing discourse and research on IBSA by applying a cyber routine activity theory (Cohen & Felson, 1979) to better understand risk factors and protective factors for this newly recognized, consequential form of cybervictimization. Below, we provide an overview of the theory before presenting our hypotheses, methods, and results.

Literature review

Routine activity theory (RAT) (Cohen & Felson, 1979) is an opportunity theory that has been applied to not only terrestrial crimes – that is, crimes that occur in the physical, real-world context (such as burglaries and assaults) but to cybercrimes and cybervictimization. Routine activity theory (RAT) consists of three major components[1]: the presence of a motivated offender, an available target (i.e., victim), and a lack of capable guardian(s) who might prevent or react to attempts at victimization (Cohen & Felson, 1979). In its initial conception, RAT was a theory wherein space and time converged to help explain criminal offending, with a focus on property crimes like burglaries. It was one's routine activities (or regular, everyday behaviors and acts) in conjunction with available opportunities that create a criminogenic environment, therein crime will occur. RAT describes victimization as occurring at the epicenter of the convergence of these three elements (Cohen & Felson, 1979).

Traditional research that applied elements of RAT often finds empirical utility in considering victimization in terms of everyday routines (with an emphasis on risky behaviors) that may position individuals to be more or less at risk of victimization. There is general support of the basic premise of RAT: people who live risky lifestyles (i.e., participating in deviant behaviors like drinking alcohol and drug-use) may experience an increased likelihood of victimization, presumably because of these risky lifestyles (Cohen & Felson, 1979; Fisher et al., 1998; Miethe et al., 1987; Mustaine & Tewksbury, 1998; Zhang et al., 2001). Relatedly, scholars have examined various cybercrimes through a RAT framework, such as online sexual harassment (Choi & Lee, 2017; Vakhitova et al., 2016; Yar, 2005), cyberbullying (Navarro et al., 2017), cyberstalking (Reyns et al., 2011), and non-consensual pornography (Henriksen, 2020). Despite these important theoretical advancements, there has not been a concentrated effort to specifically apply RAT to that of IBSA. Additionally, IBSA is often not disaggregated from other forms of cybervictimization like cyber harassment, which means it is still unclear what utility (if any) RAT has in explaining IBSA victimization.

The current study represents an exercise in theoretical application by testing the feasibility of such an approach in digital contexts. We apply RAT to better understand risk factors of, and protective factors from, IBSA victimization, by considering six specific and nuanced forms of IBSA. This study is the first such approach in IBSA-related scholarship, as we take care to separate the actions of *creation* from *dissemination*, and to be specific in how we distinguish consensually created content from forcible or coercive content. First, we offer a review of the three primary elements of RAT and explain how they have been applied to (cyber)victimization. We then present three hypotheses and analytic strategies that test RAT to increase understanding of IBSA risk in a sample of 506 18-to-24-year-old female survey respondents. Finally, we discuss the findings, their implications, and the limitations of this study.

Adapting RAT to cyberspace

In their early theorizing, Cohen and Felson (1979) hypothesized that technological progress in modern society might create novel and innovative means of deviance and victimization. Various scholars have made compelling arguments for framing cybercrimes (e.g., child pornography) similarly to physical acts of crime (e.g., sexual violence) (Grabosky, 2001; Puente & Hernández, 2022; Reyns et al., 2011). However, difficulties arise when transforming any traditionally terrestrial criminological theory to explain victimization in digital spaces, and RAT is not immune to this concern (Vakhitova et al., 2016, 2021; Yar, 2005).

In his application of RAT to general cybercrimes, Yar (2005) points out that some major tenets of RAT are not applicable to cybercrimes due to their nonphysical nature. Specifically, the convergence of time and space in cyberspace does not allow for a convergence for the victim and the offender at the same time and place (Yar, 2005). By drawing on Eck and Clarke's (2003) systems and networks, Reyns et al. (2011) argue that the convergence of victims and offenders can function continuously over time, rather than as a single instantaneous moment. Various scholars have made the same argument (Marcum et al., 2010; Mikkola et al., 2021; Näsi et al., 2017; Ngo & Paternoster, 2011; Puente & Hernández, 2022; Vakhitova et al., 2019).

Additionally, Yar (2005) maintains that the suitable target element is "more complex with similarities in respect of value but significant differences in respect of inertia, visibility and accessibility" (p. 424), meaning that three of the four sub-variables within a suitable target are lacking appropriate transposability from offline to online contexts (also see Felson & Clarke, 1998). For instance, inertia cannot be fully readapted in the digital context as digital information offers "little inertial resistance" (Yar, 2005, p. 420). Further attempts to re-conceptualize this, and other limitations in cybervictimization scholarship were undertaken by Vakhitova et al. (2016, 2022). These recent efforts maintain that when RAT's concepts are appropriately adapted and transposed, it is an adequate theory for studying cybervictimization.

Routine activity theory elements

Proximity and exposure to motivated offenders

Proximity to motivated offenders is traditionally understood as the physical space between potential victims and offenders (Cohen et al., 1981). Proximity to motivated offenders has historically been measured by place of residence, socioeconomic characteristics of the area, and perceptions of safety (Miethe & Meier, 1990). In the context of cyberspace, this principle has been defined as "being virtually present in the domains of influence of potential cyber abusers" (Vakhitova et al., 2022, p. 10). This definition is more suitable for the current study as it identifies the space in which potential victimization might occur as virtual (i.e., domains of influence) and the offenders who might victimize individuals as coalescing in these spaces. Thus, being in "virtual proximity" to motivated offenders in cyberspace means interacting with other online users, either known or unknown to the individual through chatrooms and forums (Hawdon et al., 2017). This might also encompass following or friending other users and accounts to expand one's social network, and inadvertently exposing oneself to malicious or devious account holders. In practice, allowing someone access to a personal account through the act of adding them to one's virtual friends list opens them up to potential cybervictimization.

Exposure to motivated offenders includes physical visibility and accessibility of potential victims (Cohen et al., 1981). This distinction between exposure and proximity recognizes the possibility that individuals may have an increased proximity to motivated offenders, but have low exposure to crime, subsequently affecting one's differential risk of victimization (Cohen et al., 1981; Miethe & Meier, 1990). In a digital context, exposure can be understood as the visibility and accessibility of the potential victim that is evident through their digital activities (Vakhitova et al., 2022). Both visibility and accessibility are often associated with time spent online or the quantity of various engagement in online activities, such as social networking sites (SNS) and social media accounts (Marttila et al., 2021). As mentioned previously, the concept of exposure has not always been analyzed separately from or in addition to the concept of proximity.

Target suitability or attractiveness

Target suitability suggests that the potential victim offers an offender some value or benefit (Miethe & Meier, 1994). Recent RAT examinations of cybervictimization tend to use some combination of proxy measures of risk and risky behaviors to operationalize target suitability. Proxy measures like gender, sexual orientation, race, and/or relationship status are often used as indirect measures of the expected outcome and should closely be related to the primary variable of interest (Holt et al., 2016; Reyns et al., 2011). Scholars argue for the use of demographics as measures of target suitability primarily because certain demographic factors (e.g., age, gender, race) are indeed related to the risk of some types of victimization (Popp, 2012), while others caution against using proxy measures (Mustaine & Tewksbury, 1998) since they do not directly measure the qualities that might affect the motivated offender's perception of the individual as a vulnerable target (Popp, 2012).

Secondly, various "risky" behaviors have been proposed as behaviors that make a potential victim appear "attractive" or "suitable" for cybervictimization. These behaviors include sexting, browsing risky content, other online forms of deviance, and posting information online (Holt & Bossler, 2009; Näsi et al., 2017; Räsänen et al., 2016; Reyns et al., 2011). These risky behaviors are used to approximate target suitability because they purportedly attract the attention of motivated offenders and increase one's blameworthiness for the victimization because of their own participation in risky activities (Mustaine & Tewksbury, 1998).

(Lack of) capable guardianship

Guardianship is understood as the ability of persons or objects in preventing crime (Cohen et al., 1981). The lack of adequate guardianship creates the conditions and opportunity for targeting (Reynald, 2011). Capable guardianship may include direct (physical presence) or indirect (use of security camera) means (Miethe & Meier, 1994); for instance, certain people like neighbors, bystanders, and law enforcement officers may be able to intervene and serve as adequate guardians against victimization. Hollis et al. (2013) argue that guardianship *requires* a human element that exists outside of oneself to identify danger and prevent victimization, and that the guardian and the target cannot hold the same role.

Other measures of guardianship include various physical features such as security locks, security alarm systems, and personal protection devices like mace can function as tools of guardianship (Cohen et al., 1981; Vakhitova et al., 2016). On the other hand, some scholars maintain that target hardening measures (e.g., security locks, personal protection devices) are more in line with target suitability, rather than a true measurement of capable guardianship, since these behaviors attempt to lessen one's *attractiveness* for victimization (Hollis et al., 2013). Mustaine and Tewksbury (1998) define capable guardianship as offering a "degree of protection afforded to property and persons" (p. 834) without a further qualification of who or what is responsible for protecting in the first place.

In cyberspace, guardianship has been operationalized as one's tech savvy skills to promote security, which can also be defined as self-guardianship (Vakhitova et al., 2022). This includes regularly changing passwords on social networking sites, installing various security and firewall features to identify hacking attempts, and general online risk awareness, which enables the user to protect themselves against victimization (Leukfeldt & Yar, 2016). Indeed, as Sampson et al. (2010) stated, "most guardianship is self-guardianship" (p. 46). In critique of self-guardianship, other researchers maintain that this extension is a troubling departure from the original theoretical foundation, which argues that self-guardianship is indistinguishable from target suitability, and that there is a fundamental theoretical distinction to be made between self-protection and external forces of guardianship (Hollis et al., 2013; Vakhitova et al., 2022). In sum, the lack of consistent definitions and measurement of capable guardianship across traditional approaches (Hollis et al., 2013; Mustaine & Tewksbury, 1998; Sampson et al., 2010) also affects its transposability to digital contexts (Vakhitova et al., 2022)

While we recognize that the RAT literature, and its former variants like lifestyle exposure theory (Hindelang et al., 1978), is limited due to these measurement and theory specification issues, we seek to adhere as closely as possible to the original definitions and conceptualizations of the three main elements of RAT to maintain theoretical parsimony. For the purposes of the current study, proximity/exposure to motivated offender is conceptualized as those factors that make a target more *visible* and *accessible* to the offender. Target suitability is defined as offering *symbolic value* to the offender and capable guardianship is understood as self-guardianship behaviors that create *opportunity* for victimization.

Empirical studies of routine activity theory in cyberspace

Researchers have focused on applying RAT (or its integrated cousin, LRAT) to various cybercrimes like cyberbullying, cyber harassment, and cyberstalking (e.g., Choi, 2008; Choi & Lee, 2017; Leukfeldt & Yar, 2016; Marcum, 2009; Marcum et al., 2010; Navarro et al., 2017; Puente & Hernández, 2022; Reyns et al., 2011; Vakhitova et al., 2016, 2019; Vale et al., 2022; Yar, 2005). For instance, Marcum (2009) investigated how undergraduate college students use the Internet and how their relationship with cyberspace impacts their risk of online victimization (e.g., incidents involving unwanted non-sexual harassment, unwanted exposure to sexual material, and solicitation for sexual activity), by applying a routine activity theoretical framework. The author finds strong support for RAT, with target suitability offering the largest effect on the dependent variables of online victimization, which was operationalized by various online actions that made one more or less accessible to a potential motivated offender: personal information posted on social networking sites, using a non-privatized network, communicating with others online, and sharing personal information to someone online (Marcum, 2009).

In a similar study relying on data from undergraduate student surveys, Reyns et al. (2011) find empirical support for RAT in the context of cyberstalking. They find that greater target attractiveness, measured as self-disclosed information like one's full name and relationship status, was associated with cyberstalking risk (Reyns et al., 2011; also see; Choi, 2008). They operationalized online guardianship as online peer deviance, which was significantly associated with cyberstalking victimization. Overall, Reyns et al. (2011) find that target attractiveness and guardianship had moderate effects on cyberstalking, but exposure and proximity (which was measured by variables like spending time online, number of followers, and frequency of updating social networking accounts) were found to have the weakest relationships with this form of victimization. Vakhitova et al. (2019) also assessed various lifestyle and RAT tenets in an examination of broad types of cyber abuse, including harassment and stalking. Their measurement of target suitability includes respondent's online participation in chat rooms and self-promotion, which increased their visibility for victimization.

More recently, Vale et al. (2022) employ a similar approach in understanding risk factors associated with cyber harassment in a sample of Portuguese adolescents, and they conclude that a *lifestyles*-integrated RAT model provides sufficient utility in its application. However, their operationalization of motivated offender relied on only specific technology use, rather than on the activities that one does using those technologies. They also did not consider peer deviance as either proximity to motivated offender nor lack of capable guardianship, instead focusing their efforts on capable guardianship as it relates to parental monitoring and supervision (Vale et al., 2022). Moreover, Puente and Hernández (2022) assess similar experiences of cyber abuse in Colombian students by testing RAT. Their measurement of *capable guardianship*, which was measured by parental controls and connection between private devices and public networks, had the least explanatory power.

In sum, prior research suggests that adapting RAT to the virtual medium is feasible. However, inconsistent measurement and support makes it difficult to judge the utility of an RAT approach in cybervictimization scholarship, and the behaviors and experiences that are captured under the broad conceptualizations of cybercrime and cybervictimization are not specific enough to make specific recommendations about combatting these occurrences. To date, only one study has used elements of RAT to focus on one facet of IBSA: nonconsensual pornography (NCP), which is defined by the author as initially consensually shared with someone, but then images or video were shared with other people without their permission. In considering what kinds of risky behaviors increase the risk of victimization, Henriksen (2020) reports that engaging in sexting with peers, being filmed nude, and posting frequently (their measures of target suitability) were strongly, positively associated with nonconsensual pornography victimization. Despite this important contribution, Henriksen (2020) only considers IBSA materials that were initially created with the victim's consent, whereas IBSA can also occur when images or videos are obtained *without* the victim's consent.

The current study

In furthering these efforts to theoretically contribute to an understanding of RAT as it may relate to IBSA, we expect to find that individuals who (H1) interact more regularly with potential motivated offenders and (H2) make more suitable or attractive targets will be more likely to have experienced IBSA victimization. Further (H3), those who engage in greater capable guardianship will be less likely to have experienced IBSA victimization. These hypotheses are informed by previous research and literature on cybervictimization that specifically aimed to test the reliability and effectiveness of RAT (Henriksen, 2020; Marcum, 2009; Reyns et al., 2011; Vakhitova et al., 2019), and measures were adapted or created to better understand protective and risk factors of IBSA victimization. Further, this study aims to improve the understanding of risk for IBSA by focusing on six specific and nuanced forms of IBSA to better understand the complicated intricacies of this form of cybervictimization.

Methods

Data and sample

The data were collected using a third-party company, Centiment (https://www.centiment.co/). This company is a comprehensive research platform that assists researchers in designing surveys, reaching an appropriate audience panel, and collecting data. Centiment recruits respondents from Facebook and LinkedIn. Respondents who desire to be directly compensated for their time must provide a verified US-based phone number and a PayPal account. Centiment asks respondents for their demographic information upon joining the overall audience panel. These demographic questions are then asked again every 30 days if that information is subject to change. Additionally, respondents do not know what answers qualify them for a survey, and they are not told the topic of the survey before opening the informed consent document, decreasing the likelihood of self-selection based on the nature of the survey. They are simply provided with the estimated time it will take to complete the survey and the financial compensation they can earn before they decide to participate.

Centiment ensures the quality of data by returning only fully completed surveys without missing data and the inclusion of attention-check questions to ensure participants are reading the questions before answering. The sampling frame included females between the ages of 18 and 24 years old. This was established based on prior literature that finds this category of individuals is at high risk for online victimization, such as IBSA (Eaton et al., 2022; Henry et al., 2021; Ruvalcaba & Eaton, 2020; Tamarit-Sumalla et al., 2022). The desired sample size was 500, and Centiment returned 506 completed surveys. Demographic information for this sample is listed in Table 1.

Measures

Dependent variables

The dependent variables in this study include six measures of IBSA. These items include: (1) *creation of media*, (2) *dissemination of media*, (3) *threatening to create or disseminate media*, (4) *creation of media depicting unwanted sexual experiences*, (5) *dissemination of media depicting unwanted sexual experiences*, and (6) *sextortion* (see Table 2 for the wording of each item). Survey respondents were presented with definitions for each of these terms. Unwanted sexual experience was defined as a range of behaviors such as sexual harassment, sexual abuse, assault, rape, and the threat of such behaviors. Though some of these terms are not mutually exclusive, the use of the word "unwanted" indicated an element of non-consent in the IBSA experience. These items were based on prior literature that used similar measures (Champion et al., 2022; Gámez-Guadix et al., 2022; Pedersen et al., 2022; Powell & Henry, 2019; Ruvalcaba & Eaton, 2020).

Respondents were asked "Have any of the following happened to you, personally, online when you were at least 18 years old or older?" and their response options included "Never," "At least once," "2–3 times," "4–5 times" or "More than 5 times" for each item. These responses were averaged into a single variable of IBSA experiences (Cronbach's $\alpha = .92$).

Table 1. Demographic characteristics of participants (*N* = 506).

	M	*SD*	*n*	%
Demographic category				
Age	21.03	2.06		
Gender identity				
Woman			477	94.27
Genderqueer or non-binary			15	2.96
Man			4	0.79
Transgender Woman			3	0.59
Sexual identity				
Heterosexual			330	65.22
Bisexual			89	17.59
Lesbian			26	5.14
Pansexual			21	4.15
Asexual			13	2.57
Gay			7	1.38
Hispanic or Latina				
No			387	76.48
Yes			119	23.52
Racial identity				
White			281	55.53
People of color				
Black or African American			118	23.32
Asian or Asian American			45	8.89
Two or more races			43	8.50
American Indian/Alaska Native			10	1.98
Native Hawaiian/Pacific Islander			9	1.78
Education level				
High school graduate			178	35.18
Some college credit, no degree			152	30.04
Two or four year degree			99	19.57
No schooling completed			41	8.10
Post-graduate degree			26	5.14
Trade or vocational training			10	1.98
Relationship status				
Single			231	45.65
Committed relationship (not married)			146	28.85
Casually dating			76	15.02
Committed relationship (married)			53	10.47
Living situation				
I live with family members			236	46.64
I live with romantic partner			121	23.91
I live alone			76	15.02
I live with roommates			73	14.43

Total sample size = 506; 5 participants selected "Other" for their sexual identity and 15 participants selected "Prefer not to say;" 7 participants selected "Other" for their gender identity.

Independent variables

The independent variables include measures of the three key elements of routine activity theory (RAT): motivated offenders, suitable target, and guardianship.

Motivated offender

The motivated offender concept is measured using 13 total items. Relying on an earlier defined readaptation of motivated offender as the visibility and accessibility of the potential victim that is evident through their digital activities within their "domains of influence" (Vakhitova et al., 2019, p. 228), these measures were selected due to their ability to make a potential target more visible and accessible.

Table 2. Frequency of victimization by IBSA type.

		At least	2–3	4–5	More than
	Never	once	times	times	5 times
IBSA Type	*n*, (%)	*n*, (%)	*n*, (%)	*n*, (%)	*n*, (%)
(1) Creation of media A nude or seminude image/video of you was taken without your permission.	385, (76)	67, (13)	32, (6)	15, (3)	7, (1)
(2) Dissemination of media A nude or seminude image/video of you posted online or sent to others without your permission.	400, (79)	58, (11)	33, (6)	8, (1)	7, (1)
(3) Threatening to create or disseminate media	389, (77)	63, (12)	36, (7)	12, (2)	6, (1)
(4) Creation of media depicting an unwanted sexual experience (USE)	400, (79)	59, (12)	30, (12)	10, (2)	7, (1)
(5) Dissemination of media depicting an unwanted sexual experience (USE)	412, (81)	47, (9)	24, (5)	15, (3)	8, (1)
(6) Sextortion Been threatened to have a nude image/video of you exposed online in exchange for money, sexual favors, or the production of other nude media of you.	396, (78)	61, (12)	30, (6)	14, (3)	5, (1)

First, respondents are asked "In an average day, how much time do you spend online doing the following activities: using *dating applications*, visiting *pornographic websites*, *gaming*, and *social networking sites*. Response options for time spent doing these activities included a range of hours: 0 hours, 1–2 hours, 3–5 hours, 6–9 hours, 10+ hours.[2] Additionally, sending sexually explicit images and/or videos (i.e., sexts) to a variety of individuals such as a romantic partner, strangers, dating or hookup partners, friends, or acquaintances is hypothesized as increasing one's proximity to a motivated offender as this may potentially increase one's closeness to a perpetrator. *The number of people to whom explicit media is sent* (in one's lifetime) is summed into a single measure (Cronbach's $\alpha = .81$).[3]

Two additional variables were used to measure proximity to motivated offenders: *offline interactions with people met online* and *offline sexual interactions with people met online*. The response options for these two variables were binary: yes or no.

Finally, *proximity to known offenders* is measured as a single measure, averaging responses to three peer behaviors: peers engaging in cyber harassment, image-based sexual abuse perpetration, and sexting (Cronbach's $\alpha = .74$). Response options included answering "All of them," "most of them," "some of them," "none of them" to the question "how many of your friends have engaged in [type of behavior]?"[4]

Target suitability

Target suitability is measured by a question that asks "What, if any, personal information about you is publicly accessible to people online?." We conceptualized target suitability as presenting a potential offender some perceived value (symbolic or otherwise) or benefit, so that targeting this victim is feasible and attractive (Miethe & Meier, 1994; Vakhitova et al., 2016). In other words, there must be some quality about the target which makes accessing it/them desirable to an offender; thus, publicly accessible information about a potential victim provides qualitative context about the victim to the offender.

Respondents were directed to "check all that apply," and they selected any (or none) of 12 types of information. This information includes full name, phone number, public e-mail, address, work or school location, public relationship status, public sexual identity, links to social networking accounts, interests, photos of self, videos of self, and live location tagging (Cronbach's α = .67). These 12 dichotomous items were summed into a single measure of target suitability.[5] Since individuals can potentially increase their attractiveness to a motivated offender based on the various exposure or accessibility of their personal information (such as through revealing their relationship status online), this measure of target suitability is used in the present study.

Self-guardianship

This concept is operationalized by six measures of password protective behaviors and the number and nature of participants' online accounts. Keeping in mind that guardianship suffers from chronic misrepresentation in empirical research, we have chosen to conceptualize this element as one that enables users to protect themselves against digital victimization, thus limiting the opportunity for victimization (Vakhitova et al., 2022).

Respondents were asked whether they utilize *dual security authentication* across social networking sites, if *anyone else knows the password to social networking sites* or *password to their device*, whether they have *public accounts*, *number of social networking accounts*, and *number of followers*. These six variables were entered as individual variables.[6] These guardianship questions were not presented to respondents who indicated they did not have any social networking accounts ($n = 24$, 4.74% of the sample), who were coded 0 on those variables. This was done in order to maintain the entire sample; removing people with systematically missing data could lead to false assumptions and conclusions about risk factors for IBSA.

Control variables

We control for sexual identity (1 = LGB+), as sexual minorities experience higher rates of technology-facilitated sexual abuse and harassment than heterosexual women (Eaton et al., 2022; Powell et al., 2020, 2022; Tamarit-Sumalla et al., 2022), and race (1 = people of color), as people of color experience higher rates of cybervictimization than their white counterparts, often in tandem with race-based harassment and abuse (Kowalski et al., 2020; Lenhart et al., 2016).

Control variables also include relationship status (1 = partnered), living situation (1 = lives alone), and education level (1 = college degree or higher), since prior research suggests that unpartnered individuals and highly educated individuals are more likely to be victims of various forms of digital abuse and scams (Whitty, 2015). However, these variables were collected in reference to the time of data collection, and we did not ask about their relationship, living, or education statuses *at the time of* their victimization.

Analytic strategy

Following Tabachnik and Fidell's (2013) recommendation on calculating the required sample size: $N > 50 + 8$ m (m = number of independent variables, which is 17 in this study), 186 is the minimum number of cases that is required in the sample size. Since the current study meets this threshold with 506 cases, the following regressions can be conducted with the appropriately sized sample. The hypotheses are first tested by conducting

Table 3. Binary logistic regression analysis comparing victims and non-victims of IBSA.

Independent variable	*OR*	95% CI
Motivated offender		
Time spent online	1.900***	[1.308, 2.759]
Offline interactions with online individuals	1.005	[0.573, 1.762]
Offline sexual interactions with online individuals	1.2478	[0.723, 2.266]
Number of individuals sexual media shared with	1.541***	[1.301, 1.826]
Proximity to motivated offenders scale	3.542***	[2.331, 5.383]
Target suitability		
Posted/available personal information online	1.027	[0.939, 1.123]
Self-guardianship		
Dual security	1.405	[0.742, 2.660]
Number of SNS accounts	0.890	[0.739, 1.072]
Number of followers on SNS	0.827	[0.664, 1.029]
Public accounts	1.120	[0.904, 1.388]
Anyone know password to device	1.511	[0.884, 2.585]
Anyone know password to SNS	1.148	[0.586, 2.250]
Control		
People of color	1.237	[0.766, 2.000]
LGB+	0.965	[0.583, 1.588]
Single	1.537	[0.938, 2.517]
Living alone	0.897	[0.452, 1.781]
College degree	0.840	[0.489, 1.442]
Constant	0.032***	[0.008, 0.128]
−2 log likelihood	−235.520	
Model χ^2	197.46***	
Cox-Snell R^2	0.323	
McFadden's R^2	0.295	
Nagelkerke R^2	0.441	

N = 506. CI = confidence interval for odds ratio (*OR*). **p* < .05. ***p* < .01. ****p* < .001.

binary logistic regressions that compare victims and non-victims of *overall* IBSA victimization. A single dichotomous variable is created to differentiate between victims and non-victims of every type of IBSA: 1 if they *experienced one or more types of IBSA* and 0 if they *never experienced any of these types of IBSA* (Table 3).

Second, a series of logistic regressions are conducted on each of the six types of IBSA to better explore the nuanced differences across different forms of IBSA victimization between victims and non-victims of each type of IBSA (Table 4). A dichotomous variable was included for each of the six forms of IBSA in which respondents were coded 1 if they *experienced one or more incidences of that type of IBSA* and 0 if they *never experienced that type of IBSA*. This will allow for a comparison between victims and non-victims of each of the six types of IBSA. Assumptions were checked prior to running analyses; all analyses were conducted using Stata/BE version 18.0.

Results

Demographics

Overall, the sample consisted mostly of women (94.27%) who identified as heterosexual (65.22%).[7] The majority of respondents did not identify as Hispanic/Latina (76.48%) and

Table 4. Binary logistic regression analyses comparing victims and non-victims of six types of IBSA.

			Threaten	Create	Share	
	Create IBSA	Share IBSA	IBSA	USE	USE	Sextortion
Independent variable	*OR*	*OR*	*OR*	*OR*	*OR*	*OR*
Motivated offender						
Time spent online	1.900***	1.781**	1.456	1.928***	2.235***	1.612*
Offline interactions with online individuals	1.501	1.377	.924	.990	.975	1.081
Offline sexual interactions with online individuals	1.222	1.898	1.353	1.793	1.634	1.843
Number of individuals sexual media has been shared with	1.392***	1.461***	1.489***	1.253**	1.169	1.210**
Proximity to motivated offenders average	2.450***	2.589***	2.740***	2.541***	2.504***	3.203***
Target suitability						
Posted personal information online	0.958	1.031	0.965	1.016	1.008	1.040
Self-guardianship						
Dual security	1.183	0.987	1.422	1.847	1.454	1.293
Number of SNS accounts	0.885	0.845	0.933	0.839	0.786*	0.924
Number of followers on SNS	0.918	0.811	0.763*	0.843	0.836	0.818
Public accounts	1.309*	0.996	0.913	0.968	1.097	0.994
Anyone know password to device	1.186	1.175	2.062*	1.300	1.269	1.153
Anyone know password to SNS	1.248	1.644	0.928	1.028	1.676	1.034
Control						
People of color	1.381	0.837	0.955	1.079	0.839	0.792
LGB+	1.004	0.658	1.177	0.723	0.837	1.184
Single	1.241	1.380	1.387	1.140	1.187	1.762*
Living alone	0.761	0.600	0.678	0.815	0.601	0.695
College degree	1.016	0.807	0.643	0.762	0.878	0.818
Constant	0.018***	0.028***	0.040***	0.035***	0.023***	0.028***
−2 log likelihood	−207.300	−186.745	−206.052	−199.185	−182.071	−194.781
Model χ^2	142.1***	145.9***	135.1***	121.1***	121.6***	140.3***
Cox-Snell R^2	0.245	0.251	0.234	0.213	0.214	0.242
McFadden's R^2	0.255	0.281	0.247	0.233	0.250	0.265
Nagelkerke R^2	0.367	0.390	0.355	0.332	0.346	0.373

N = 506. *OR* = odds ratios. *p < .05. **p < .01. ***p < .001.

most identified as white (55.23%). The average age is 21.03 years old, and ranges from 18 to 24. Approximately 35% of the sample were high-school graduates; 46% were not in a relationship; and 47% lived with family members. For an overview of the sample characteristics, see Table 1.

Descriptive statistics

Of the 506 survey respondents, approximately 24% experienced the creation of IBSA media, 21% experienced the dissemination of media, 21% had media created depicting an unwanted sexual experience (USE), and 18.6% had media of an USE disseminated. Approximately 23% of respondents reported being threatened with the dissemination of IBSA media, and 21.7% experienced *sextortion*, or sexual extortion. Seventy-three respondents (14%) respondents reported experiencing *every* form of IBSA.

Comparing victims and non-victims of IBSA

A binary multiple logistic regression analysis was conducted to estimate the probability of having experienced IBSA from 12 theoretical independent variables and five control variables. The dependent variable is binary, with 1 coded as experiencing at least one form of IBSA once or more and 0 coded as not having had any experiences with IBSA. The independent variables are the RAT variables: motivated offender, suitable target, and capable guardianship. Indicator coding was used for the following control variables: people of color, LGB+, marital status (1 = single), living alone, and having a college degree.

The log-likelihood ratio chi-square test statistic for the full model is LR $\chi^2(17) = 197.46$, $p < .001$, indicating that the overall model with all the independent variables was significant. The Hosmer–Lemeshow statistic indicated a non-statistically significant χ^2 (521.49, $p = .12$), which suggests an adequate fit of the overall model (Acock, 2023). The pseudo R^2 is 0.295. Nagelkerke R^2 indicated approximately 44.1% of the variance in IBSA experiences was accounted for by all of the independent variables.

Motivated offender (H1)

Three motivated offender variables reached statistical significance at the $p < .001$ level: time spent online ($OR = 1.900$), sexting behaviors ($OR = 1.541$), and proximity to motivated offenders ($OR = 3.542$). For each one-unit increase of time spent online doing various activities (e.g., using social media, visiting pornographic websites, gaming online, and using dating apps), the odds of having experienced IBSA increases by a factor of 1.900, or 90%.

For every person that a respondent sends a sexual image or video to (i.e., nudes/sexts), the odds of having experienced IBSA increases by a factor of 1.541, or 54.1%. Finally, proximity to motivated offenders as measured by three peer behaviors (sexting, cyber harassment, and IBSA perpetration) was also identified as statistically significant. Having more peers who engage in these behaviors increases the odds of having experienced IBSA by a factor of 3.542, or approximately 254.2%.

Examining specific types of IBSA

Binary logistic regressions were conducted to estimate the probability of experiencing six different types of IBSA from the same variables used in the first analysis.

Motivated offender (H1)

When regressing the dichotomous IBSA variables (i.e., six types of IBSA) on the RAT and control variables, a few statistically significant ($p < .001$) patterns emerge regarding motivated offenders (Hypothesis 1) (Table 4). First, *time spent online* was found to be statistically significant across several IBSA types: creation of IBSA media ($OR = 1.901$), creating media depicting sexual assault or unwanted sexual experiences ($OR = 1.924$), and sharing media depicting sexual assault or unwanted sexual experiences ($OR = 2.244$). Second, *sexting* is statistically correlated ($p < .05$) with five forms of IBSA: creation ($OR = 1.398$) and sharing of nude media ($OR = 1.477$) and the threatening to do so ($OR = 1.501$), creation of media depicting sexual assault ($OR = 1.263$) and sextortion ($OR = 1.304$).

Third, *proximity to motivated offenders* was consistently statistically significant across every single IBSA model at the $p < .001$ level: creation of IBSA media ($OR = 2.465$), sharing IBSA media ($OR = 2.615$), threatening to share IBSA media ($OR = 2.771$), creating media depicting sexual assault or unwanted sexual experiences ($OR = 2.629$), sharing media depicting sexual assault or unwanted sexual experiences ($OR = 2.560$), and sextortion ($OR = 3.228$).

Self-guardianship (H3)

Some of the capable guardianship variables were statistically significant at the $p < .05$ level. *Number of social networking accounts* is correlated with having media shared that depicts unwanted sexual experiences ($OR = 0.786$). The *number of followers on social networking accounts* ($OR = 0.763$) and *anyone knowing password to device* ($OR = 2.062$) is correlated with being threatened with the sharing of IBSA media. Having *public accounts* is correlated with the creation of IBSA media ($OR = 1.309$).

In sum, we find some support for the hypothesis that IBSA is positively correlated with exposure and proximity to motivated offenders (H1) and negatively associated with capable guardianship (H3). However, we do not find support for a link between IBSA and target suitability (H2).

Discussion

Though applying a cyber routine activity theory (RAT) framework to cybervictimization has been attempted by several scholars (Choi & Lee, 2017; Holt & Bossler, 2009; Leukfeldt & Yar, 2016; Marcum et al., 2010; Reyns et al., 2011; Vakhitova et al., 2019; Vale et al., 2022; Wolfe et al., 2016), the current study is one of the first attempts of doing so to the specific type of cybervictimization: image-based sexual abuse (IBSA) (also see Henriksen, 2020). The present study contributes to these ongoing theoretical endeavors by articulating the significance of theoretical integration to explain cybervictimization. IBSA is a technology-driven form of abuse that is often entangled in broader social constructs of classism, racism, sexism, and homophobia. It is becoming increasingly more difficult to identify victims, perpetrators, and the complicated context in which these harms occur. This is particularly difficult to achieve due to the nature of the internet which affords online users' anonymity, sense of protection, and invisibility that makes it easier and more accessible to commit such harmful acts. By understanding what makes individuals vulnerable to IBSA victimization, we can better inform policy, prevention, and intervention strategies that address specific types of IBSA.

The current study finds several statistically significant associations between RAT variables and IBSA victimization. There is partial support for H1, which proposed that individuals who interact more regularly with motivated offenders (through exposure and proximity) are at a higher risk of experiencing IBSA victimization. Proximity to motivated offenders, measured by three separate peer behaviors (sexting, cyber harassment, and IBSA perpetration), was consistently statistically significant when comparing IBSA victims to non-victims in the overall model and across every one of the six specific forms of IBSA.

These findings further support prior scholarship that operationalized proximity to motivated offender as a measurement of peer deviance and criminality in both terrestrial (Jensen & Brownfield, 1986; Lauritsen et al., 1992; Sampson & Lauritsen, 1990; Zhang et al., 2001) and cyber contexts (Bossler et al., 2012; Holt & Bossler, 2009; Marcum, 2009; Marcum et al., 2010; Vale et al., 2022; Wolfe et al., 2016). Based on decades of research, it appears that associating with delinquent peers, or having friends who engage in deviant behaviors, increases one's exposure to potential offenders in their lives.

Situating deviant peers as motivated offenders, though not necessarily a novel finding within cybervictimization and RAT scholarship, does offer a unique perspective within terrestrial research through a cyber victimological lens. Though one of the main critiques of RAT's applicability to explaining cybervictimization is that it does not do enough in addressing the motivated offender aspect of interpersonal acts of violence, such as sexual assault, the current study finds that it indeed matters a great deal who the victim engages with (i.e., delinquent peers). It is readily understood across victimization literature that individuals, particularly women, are more likely to be victimized by people they know, rather than strangers (National Incident-Based Reporting System [NIBRS], 2011). This contention provides one potential explanation for this finding in the present study.

These results suggest that association with deviant peers heightens one's risk of being victimized. While some research does find that one's deviant peers are the ones engaging in physical sexual assault against those reporting higher risk (Schwartz & Pitts, 1995; Stogner et al., 2014), this is not necessarily the case. It may be that deviant peers are unable to offer guardianship against IBSA if they too engage in these very behaviors, potentially because they may view them as unproblematic or irrelevant. Further, understanding one's risk of IBSA victimization as associated with deviant peers presents the possibility of extending RAT to include tenets of social learning theory, which emphasizes differential association and reinforcement as related to offending (Akers & Jensen, 2010; Curry & Zavala, 2020). Clearly, the victim's relationship with their social networks is an important consideration in cybervictimization scholarship.

Research indicates that as people spend more time online, they may be more likely to engage in risky behaviors that might increase their risk of victimization (Bossler et al., 2012; Vale et al., 2022). This is supported by the findings of the current study. Spending time online was positively associated with having experienced IBSA in three different ways: creation of IBSA media, creating media depicting unwanted sexual experiences, and sharing media depicting unwanted sexual experience. Additionally, spending *time online* was correlated with overall IBSA (all types). These are significant findings in an era when one's digital presence and digital social life is more important than ever before. Americans are spending more time online both for pleasure and for business. It is difficult to completely avoid a digital presence, so uncovering how technology and internet users can become vulnerable to cybervictimization like IBSA is vital. It is what one does online that affects their differential risk of experiencing IBSA victimization (Ngo et al., 2020). This association between spending time online doing various activities and being a victim of IBSA contends that modernized digital activities like pursuing romantic relationships through dating apps are much more normalized.

However, the very concept of risk and risky behaviors continues to evolve as behaviors that were once taboo or socially ostracized (e.g., having consensual sexual relationships between non-married individuals) are now much more socially accepted and normalized (e.g., hookup culture). These cultural and societal shifts are crucially re-defining the stringent parameters of the traditional RAT variables; thus, the current study measures these behaviors as increasing one's proximity and/or exposure to motivated offenders, but these variables may no longer be viewed or considered as inherently risky as perhaps they were 20 years ago.

Another measurement of proximity to motivated offender, *sexting*, was significantly correlated with IBSA victimization overall and for three of the six specific types: creating IBSA media, sharing of IBSA media, and threatening to share IBSA media. This finding further corroborates other research that has found sexting to be correlated with IBSA victimization (Gámez-Guadix et al., 2022; Henriksen, 2020; Marcum et al., 2021). Sexting is often considered a risky behavior as it can initiate victimization even if the initial act (sending a sexual message or image) was consensual in nature (Gassó et al., 2020; Rollero et al., 2023; Shapiro et al., 2017). Moreover, in the same way that sexually aggressive men may view women who drink alcohol or use drugs as potentially suitable targets because of their exposed vulnerability (Schwartz et al., 2001), women who consensually send a nude image of themselves as part of a healthy and normal sexual and/or romantic behavior, may also be viewed by perpetrators of IBSA as appropriate targets. This warrants a prevention program that directs its awareness efforts within dating site platforms. For instance, Bumble, a women-friendly dating application, emphasizes an Enforcement Philosophy wherein users must adhere to the mission of kindness, safety, and inclusivity by being held accountable for various forms of harassment, sexual and physical violence, and cyberbullying (Bumble.com, 2024). Such efforts would be enhanced by requiring all application users to complete anti-sexual harassment training prior to accessing its content.

Target suitability was measured by the number of types of personal information that respondents post, and it was not significant in any of the models. Thus, there is no support for H2, which proposed that adequate and/or sufficient target suitability would increase one's likelihood of experiencing IBSA victimization. Namely, it might be worthwhile to consider the difference between *posting* (as it was conceptualized in the current study) and *sharing* personal information. It may be that the additional act of intentionally providing potentially motivated offenders information about oneself is what makes it easier for perpetrators to locate or target their victims.

Further, very few of the variables used to operationalize self-guardianship were statistically significant. Hypothesis 3 proposed that guardianship, as operationalized by technology use, social media use, and self-guardianship measures like dual-security systems and use of password protection, will increase one's risk of experiencing IBSA victimization. The *number of social networking accounts* and *number of followers on social networking accounts* were found to have the opposite relationship. One possible explanation for this finding is that creating and deleting multiple social networking accounts makes for a "moving target," as in the potential victim, does not provide sufficient digital stability in their online presence to be victimized.

Additionally, having *public accounts* and *someone knowing the password to one's device* were correlated with two types of IBSA, which does support the expected relationship between these self-guardianship measures and IBSA victimization. For instance, social networking accounts that are public (versus private) increase the odds of experiencing the creation of IBSA materials by 30.9%. A public account means that followers and strangers alike may access and engage with any element of one's social digital profile, indicating increased vulnerability for this specific type of IBSA victimization.

Though the traditional principle of RAT assumes that guardianship should be considered with both *social* and *physical* parameters, the current study did not make such a distinction. The present results indicate that the capable guardianship premise of RAT may benefit from explicit consideration of *both* social and physical parameters; this omission can possibly explain the lack of strong support for this RAT element. Additionally, guardianship was measured as self-guardianship without a consideration of external protectors, controllers, handlers, or enforcers, as is outlined by the original (and subsequent variants) of RAT (Hollis et al., 2013; Reynald, 2011; Sampson et al., 2010). Further items should be developed to capture external guardianship as separate from self-guardianship, which is arguably reminiscent of target suitability, further devolving consistency in theoretical operationalization.

Limitations

A number of limitations in the current study warrant mention. Because the current study utilized a non-probability convenience sampling strategy, wherein the target sample of the current study was drawn from an online sample of participants sourced from an online panel, there are limits regarding generalizability, social desirability biases, external validity, and recall concerns (McEwan, 2020). Due to Centiment's use of recruitment via social media platforms (e.g., Facebook, LinkedIn), there are concerns around self-selection biases, which could have had an unintentional effect on the findings. Additionally, while Centiment relies on social networking sites to recruit their audience pool, it is unclear why 24 respondents in our sample indicated not having social networking accounts. We propose that participants do not *necessarily* come from social media platforms as Centiment recruits their audience panel from a variety of sources, including social media and partner networks. We also did not define "social networking account/site" or "social media account" so some may not consider LinkedIn necessarily "social media," for instance. We also leave some explanatory room for human/user error and recognize that participants may have selected an incorrect or wrong answer.

Furthermore, social desirability biases exist in many, if not most, survey designs and the current study is not immune to this concern. Since this study examines a sensitive and potentially re-victimizing topic, it is possible that respondents may have misreported their responses (Krumpal, 2013). It is also noted that many victims of IBSA minimize and trivialize their experiences, particularly if they have also experienced offline physical and sexual violence (Bates, 2017; Powell et al., 2022). IBSA then, in relation to physical and sexual violence, may be viewed by the victim as "not as bad" or "not as serious" as offline violence. This minimization is akin to the ways in which victims of physical and sexual victimization sometimes normalize and minimize their experiences as a coping or avoidance strategy (Sinko et al., 2021). Social desirability biases can be reduced in sensitive surveys such as this one by conducting validation or comparative studies, as well as framing sensitive questions in neutral ways (Krumpal, 2013).

There are a multitude of issues in the operationalization of traditional RAT variables in an IBSA context. It became evident that relying on measures from prior cybervictimization scholarship is not an effective approach in examining IBSA specifically. We suggest that target suitability measured by the information and knowledge that is available about a target must represent symbolic value and benefit to the offender beyond intangible information on the internet. Image-based sexual abuse includes an interpersonal element that must be accounted for if we intend on theorizing about one's differential risk of being targeted. This may include queries surrounding consensual sexting behaviors, communication with strangers via online platforms, contextual information about the victimization (e.g., who was the perpetrator) and digital routine activities that go beyond *visibility*.

Finally, the relationship between routine activities and IBSA victimization cannot be assumed as causal nor in the hypothesized direction (i.e., online behaviors impacting IBSA victimization). Our data were cross-sectional; respondents were asked to identify experiences and behaviors at one point in time. It is possible that past IBSA victimization experiences were driving the online behaviors of victims rather than the reverse, and research in which respondents are asked about their experiences at multiple times with repeated measures could help elaborate on the relationships between our concepts.

Future directions

It is worthwhile to consider the ways in which this study and future research stemming from IBSA scholarship can improve. First, two of RAT's main criticisms are its focus on victims, which can be perceived as victim-blaming, and its lack of consideration of gender and broader structural sociological concepts that play an important role in victimization risk (i.e., gender-blind) (Henry et al., 2021; Mustaine & Tewksbury, 2002; Schwartz & Pitts, 1995). Though RAT is useful in identifying specific risk factors for IBSA victimization (i.e., proximity to deviant peers, sexting, and spending time online), it does not fully address the sociocultural or macro-level causes of this type of victimization (Henry et al., 2021).

Indeed, many victims of IBSA are targeted *because* of who they are (i.e., young, female, LGBTQ+) and contextualizing these vulnerabilities within gender-based abuse and patriarchal oppression more broadly would provide a more holistic understanding of IBSA and related abuses (DeKeseredy & Schwartz, 2016; Henry & Powell, 2018). It is becoming clearer in emerging studies (Champion et al., 2022; Henry et al., 2019; Pedersen et al., 2022; Powell et al., 2022; Walker & Sleath, 2017; Wick et al., 2017) that men and women experience IBSA and other technology-facilitated abuse at comparable rates, albeit in different and unique contexts. By only examining the IBSA experiences of a narrowly specified demographic (18- to 24-year-old females), it is not possible to make comparisons based on sex or gender. It is prudent to consider these differences in victimization risk across multiple and intersectional demographic groups.

One possible avenue for future study is an emphasis on perpetrator motivation as situated in rape culture and patriarchy, much like the arguments that Schwartz and Pitts (1995) made in their model of a feminist routine activity theory. Mustaine and Tewksbury (2002) followed a similar approach by applying a feminist integration of routine activity theory to explain the sexual victimization of college women. By introducing measures of rape-supportive beliefs as part of gauging perpetrator motivation, our broader understanding surrounding the breadth and depth of IBSA can be improved (Franklin & Menaker, 2018; Gámez-Guadix et al., 2022). In the same way that negative peer support and congruence with rape-supportive beliefs has been linked to physical sexual violence against women (DeKeseredy & Schwartz, 2013; DeKeseredy et al., 2019; Powell & Henry, 2017), cyber spaces can be viewed as a means of reinforcing gender inequality (Huber, 2023; Pedersen et al., 2022). Overall, a feminist integration would greatly benefit cyber routine activity theory by examining how the *acceptance of violence and abuse* of women is relevant in explaining IBSA victimization (Henry et al., 2021; Leili, 2019; Mustaine & Tewksbury, 2002).

We also recommend that future theoretical examinations of IBSA victimization move away from applying a traditional model of routine activity theory, and instead incorporate an expanded and integrated model of cybervictimization that includes an incorporation of *lifestyles* (Choi, 2008; Henriksen, 2020; Leukfeldt & Yar, 2016; Pratt & Turanovic, 2016; Reyns et al., 2011; Vakhitova et al., 2019; Vale et al., 2022). Most cybervictimization scholarship that integrates opportunity theories have focused on shifting the emphasis onto an expanded cyber-lifestyles routine activity theory (LRAT), and we agree that future efforts should strive to incorporate this perspective in their measures and theorizing.

Conclusion

This study extends current knowledge on the theoretical application of a traditionally stringent and apolitical criminological theory, routine activity theory, to that of a cyber form of sexual victimization: image-based sexual abuse (IBSA). This study is only one of a few attempts to apply criminological theory to explain IBSA victimization. The current study confirmed some previously identified correlates of cyber victimization such as spending time online doing specific activities (Holt & Bossler 2009), peer deviance (Reyns et al., 2011), and sexting (Henriksen, 2020). Overall, we found moderate support for RAT, particularly as it relates to proximity and exposure to motivated offenders. This application of cyber RAT holds promise for future scholarship on cyber-victimization scholarship, and with improved operationalization of measures and feminist and lifestyles integration, this theoretical explanation of IBSA can offer clearer and more nuanced results.

Notes

1. We recognize that RAT is not comprehensively defined solely by these three elements and that the theory itself more broadly contains sub-categories by which offending and victimization can be explained; namely, the value, inertia, visibility, and accessibility of the potential target and further assessment of *lifestyles* as pertinent to routines, as well as the later-developed controllers, handlers, and super controllers of guardianship (Felson & Clarke, 1998; Sampson et al., 2010; Yar, 2005). It is not within the scope of this paper to address these other elements of RAT.
2. Similar measures of proximity to motivated offenders have been used in various cybercrime scholarship (Bossler et al., 2012; Marcum et al., 2010; Näsi et al., 2017; Reyns et al., 2011; Vakhitova et al., 2019). It is important to make the distinction between general time spent online and time spent online engaging in various activities. As scholars have previously suggested, it is the participation in various deviant or risky behaviors that creates the differential risk for cyber victimization (Holt & Bossler, 2009; Ngo & Paternoster, 2011).
3. Sexting is considered a risk factor of IBSA victimization as shown in prior research (Henriksen, 2020; Marcum et al., 2021; Rollero et al., 2023), although arguably, sexting could also operationalize target suitability. We decided to use sexting behaviors as a measure of motivated

offender because it is the action of sexting that makes one virtually "exposed" and proximally close to someone who may be motivated to offend in the first place.

4. Associations with deviant peers has been supported in prior scholarship as increasing one's proximity to motivated offenders (Holt & Bossler, 2009; Vale et al., 2022; Zhang et al., 2001).
5. Prior scholarship used the same or similar measure of target suitability (Henriksen, 2020; Marcum et al., 2010; Ngo & Paternoster, 2011).
6. These items were informed by prior literature that operationalized absence of capable guardianship through password protective behaviors and general technology use, which primarily encompassed self-guardianship digital practices (Henriksen, 2020; Ngo & Paternoster, 2011; Vale et al., 2022).
7. While four of the respondents selected "Male" in the self-disclosure of their biological sex, Centiment conducts verification procedures to confirm their audience panel's demographic information; thus, the selection could have been due to user error or another anomaly. We kept these four respondents in the overall sample as their exclusion did not reveal any significant changes.

Acknowledgments

Thank you to the reviewers for their insightful feedback.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This research was funded by the Division of Feminist Criminology's Larry J. Siegel Graduate Fellowship for the Study of Gender and Crime.

ORCID

Albina Laskovtsov http://orcid.org/0000-0003-1858-6217

Ethical approval and informed consent statements

Institutional Review Board approval was received June 2023 from the University of South Carolina and re-affirmed by Shepherd University in October 2024.

References

Acock, A. C. (2023). *A gentle introduction to Stata, revised sixth edition*. Stata Press.

Akers, R. L., & Jensen, G. F. (2010). Social learning theory: Process and structure in criminal and deviant behavior. In E. McLaughlin & T. Newburn (Eds.), *The SAGE handbook of criminological theory* (pp. 56–72). Sage Publications.

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

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

Branch, K., Hilinski-Rosick, C. M., Johnson, E., & Solano, G. (2017). Revenge porn victimization of college students in the United States: An exploratory analysis. *International Journal of Cyber Criminology*, *11*(1), 128–142. https://doi.org/10.5281/zenodo.495777

Campbell, J. K., Poage, S. M., Godley, S., & Rothman, E. F. (2020). Social anxiety as a consequence of non-consensually disseminated sexually explicit media victimization. *Journal of Interpersonal Violence*, *37*(9–10), NP7268–NP7288. https://doi.org/10.1177/0886260520967150

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

Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1), 308–333.

Choi, K., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, *73*, 394–402. https://doi.org/10.1016/j.chb.2017.03.061

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

Cross, C., Holt, K., & O'Malley, R. L. (2022). "If U don't pay they will share the pics": Exploring sextortion in the context of romance fraud. *Victims & Offenders*, 1–22. https://doi.org/10.1080/15564886.2022.2075064

Curry, T. R., & Zavala, E. (2020). A multi-theoretical perspective on cyber dating abuse victimization and perpetration within intimate relationships: A test of general strain, social learning, and self-control theories. *Victims & Offenders*, *15*(4), 499–519. https://doi.org/10.1080/15564886.2020.1734996

DeKeseredy, W. S., & Schwartz, M. D. (2013). *Male peer support & violence against women: The history & verification of a theory*. Northeastern University Press.

DeKeseredy, W. S., & Schwartz, M. D. (2016). Thinking sociologically about image-based sexual abuse: The contribution of male peer support theory. *Sexualization, Media, & Society*, *2*(4), 1–11. https://doi.org/10.1177/2374623816684692

DeKeseredy, W. S., Schwartz, M. D., Harris, B., Woodlock, D., Nolan, J., & Hall-Sanchez, A. (2019). Technology-facilitated stalking and unwanted sexual messages/images in a college campus community: The role of negative peer support. *Sage Open*, *9*(1), 1–12. https://doi.org/10.1177/2158244019828231

Eaton, A. A., Jacobs, H., & Ruvalcaba, Y. (2017). *2017 nationwide online study of nonconsensual porn victimization and perpetration*. Cyber Civil Rights Initiative. https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf

Eaton, A. A., & McGlynn, C. (2020). The psychology of nonconsensual porn: Understanding and addressing a growing form of sexual violence. *Policy Insights from the Behavioral and Brain Sciences*, *7*(2), 190–197. https://doi.org/10.1177/2372732220941534

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*, 1–18. https://doi.org/10.1080/15564886.2021.2022057

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity approach. In M. Smith & D. Cornish (Eds.), *Theory for practice in situational crime prevention* (pp. 7–39). Criminal Justice Press.

Felson, M., & Clarke, R. V. (1998). *Opportunity makes the thief: Practical theory for crime prevention* (Problem-Oriented Guides for Police No. 6). U.S. Department of Justice, Office of Community Oriented Policing Services. https://popcenter.asu.edu/sites/default/files/opportunity_makes_the_thief.pdf

Fisher, B. S., Sloan, J. J., Cullen, F. T., & Lu, C. (1998). Crime in the ivory tower: The level and sources of student victimization. *Criminology*, *36*(3), 671–710. https://doi.org/10.1111/j.1745-9125.1998.tb01262.x

Fisico, R., & Harkins, L. (2021). Technology and sexual offending. *Current Psychiatry Reports*, *23*(9), 1–8. https://doi.org/10.1007/s11920-021-01269-1

Flynn, A., Powell, A., Scott, A., & Cama, E. (2021). Deepfakes and digitally altered imagery abuse: A cross-country exploration of an emerging form of image-based sexual abuse. *The British Journal of Criminology*, *62*(6), 1–18. https://doi.org/10.1093/bjc/azab111

Franklin, C. A., & Menaker, T. A. (2018). Feminist routine activity theory and sexual assault victimization: Estimating risk by perpetrator tactic among sorority women. *Victims & Offenders*, *13*(2), 158–178. https://doi.org/10.1080/15564886.2016.1250692

Franks, M. A. (2017). "Revenge porn" reform: A view from the front lines. *Florida Law Review*, *69*(5), 1251–1337.

Gámez-Guadix, M., Mateos-Pérez, E., Wachs, S., Wright, M., Martínez, J., & Íncera, D. (2022). Assessing image-based sexual abuse: Measurement, prevalence, and temporal stability of sextortion and nonconsensual sexting ("revenge porn") among adolescents. *Journal of Adolescence*, *94*(5), 789–799. https://doi.org/10.1002/jad.12064

Gassó, A. M., Mueller-Johnson, K., & Montiel, I. (2020). Sexting, online sexual victimization, and psychopathology correlates by sex: Depression, anxiety, and global psychopathology. *International Journal of Environmental Research and Public Health*, *17*(3), 1–19. https://doi.org/10.3390/ijerph17031018

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles. *Social & Legal Studies*, *10*(2), 243–250. https://doi.org/10.1177/a017405

Hawdon, J., Oksanen, A., & Räsänen, P. (2017). Exposure to online hate in four nations: A cross-national consideration. *Deviant Behavior*, *38*(3), 254–266. https://doi.org/10.1080/01639625.2016.1196985

Henriksen, C. B. (2020). *Tangled webs: A test of routine activities theory to explain nonconsensual pornography victimization (Publication No. 28487124)* [Doctoral dissertation, University of Cincinnati]. ProQuest Dissertations Publishing.

Henry, N., & Flynn, A. (2019). Image-based sexual abuse: Online distribution channels and illicit communities of support. *Violence Against Women*, *25*(16), 1932–1955. https://doi.org/10.1177/1077801219863881

Henry, N., Flynn, A., & Powell, A. (2019). Image-based sexual abuse: Victims and perpetrators. *Trends & Issues in Crime & Criminal Justice*, *572*, 1–19.

Henry, N., McGlynn, C., Flynn, A., Johnson, K., Powell, A., & Scott, A. J. (2021). *Image-based sexual abuse: A study on the causes and consequences of non-consensual nude or sexual imagery*. Routledge.

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

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Ballinger Publishing Company.

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

Holt, T. J., Bossler, A. M., Malinski, R., & May, D. C. (2016). Identifying predictors of unwanted online sexual conversations among youth using a low self-control and routine activity framework. *Journal or Contemporary Criminal Justice*, *32*(2), 108–128. https://doi.org/10.1177/1043986215621376

Huber, A. (2023). 'A shadow of me old self': The impact of image-based sexual abuse in a digital society. *International Review of Victimology*, *29*(2), 155–317. https://doi.org/10.1177/02697580211063659

Jensen, G. F., & Brownfield, D. (1986). Gender, lifestyles, and victimization: Beyond routine activity. *Violence & Victims*, *1*(2), 85–99. https://doi.org/10.1891/0886-6708.1.2.85

Kowalski, R. M., Dillon, E., Macbeth, J., Franchi, M., & Bush, M. (2020). Racial differences in cyberbullying from the perspective of victims and perpetrators. *American Journal of Orthopsychiatry*, *90*(5), 644–652. https://doi.org/10.1037/ort0000492

Krieger, M. A. (2017). Unpacking "sexting": A systematic review of nonconsensual sexting in legal, educational, and psychological literatures. *Trauma, Violence & Abuse*, *18*(5), 593–601. https://doi.org/10.1177/1524838016659486

Krumpal, I. (2013). Determinants of social desirability bias in sensitive surveys: A literature review. *Quality and Quantity*, *47*(4), 2025–2047. https://doi.org/10.1007/s11135-011-9640-9

Lauritsen, J. L., Laub, J. H., & Sampson, R. J. (1992). Conventional and delinquent activities: Implications for the prevention of violent victimization among adolescents. *Violence & Victims*, *7*(2), 91–108. https://doi.org/10.1891/0886-6708.7.2.91

Leili, J. A. (2019). *Bystander intervention, victimization, and routine activities theory: An examination of feminist routine activities theory in cyber space (Purblication No. 13905099)* [Doctoral dissertation, University of South Florida]. ProQuest Dissertations Publishing.

Lenhart, A., Ybarra, M., & Price-Feeney, M. (2016, December 13). *Nonconsensual image sharing: One in 25 Americans has been a victim of "revenge porn"*. Center for Innovative Public Health Research. https://datasociety.net/pubs/oh/Nonconsensual_Image_Sharing_2016.pdf

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Marcum, C. D. (2009). *Adolescent online victimization: A test of routine activities theory*. LFB Scholarly Publishing LLC.

Marcum, C. D., Ricketts, M. L., & Higgins, G. E. (2010). Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory. *Criminal Justice Review*, *35*(4), 412–437. https://doi.org/10.1177/0734016809360331

Marcum, C. D., Zaitzow, B. H., & Higgins, G. E. (2021). The role of sexting and related behaviors to victimization via nonconsensual pornography: An exploratory analysis of university students. *Journal of Aggression, Conflict and Peace Research*, *14*(1), 43–60. https://doi.org/10.1108/JACPR-02-2021-0578

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*(6), 862–881. https://doi.org/10.1007/s12103-021-09665-2

McEwan, B. (2020). Sampling and validity. *Annals of the International Communication Association*, *44*(3), 235–247. https://doi.org/10.1080/23808985.2020.1792793

McGlynn, C., & Rackley, E. (2017). Image-based sexual abuse. *Oxford Journal of Legal Studies*, *37*(3), 534–561. https://doi.org/10.1093/ojls/gqw033

McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'revenge porn': The continuum of image-based sexual abuse. *Feminist Legal Studies*, *25*, 25–46. https://doi.org/10.1007/s10691-017-9343-2

Miethe, T. D., & Meier, R. F. (1990). Opportunity, choice, and criminal victimization: A test of a theoretical model. *The Journal of Research in Crime and Delinquency*, *27*(3), 243–266. https://doi.org/10.1177/0022427890027003003

Miethe, T. D., & Meier, R. F. (1994). *Crime and its social context: Toward an integrated theory of offenders, victims, and situations*. State University of New York Press.

Miethe, T. D., Stafford, M. C., & Long, J. S. (1987). Social differentiation in criminal victimization: A test of routine activities/lifestyle theories. *American Sociological Review*, *52*(2), 184–194. https://doi.org/10.2307/2095447

Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B. L., Savolainen, I., Sirola, A., Zych, I., & Paek, H. (2021). Situational and individual risk factors for cybercrime victimization in a cross-national context. *International Journal of Offender Therapy and Comparative Criminology*, 1–19. https://doi.org/10.1177/0306624X20981041

Mustaine, E. E., & Tewksbury, R. (1998). Predicting risks of larceny theft victimization: A routine activity analysis using refined lifestyle measures. *Criminology*, *36*(4), 829–857. https://doi.org/10.1111/j.1745-9125.1998.tb01267.x

Mustaine, E. E., & Tewksbury, R. (2002). Sexual assault of college women: A feminist interpretation of a routine activities analysis. *Criminal Justice Review*, *27*(1), 89–123. https://doi.org/10.1177/073401680202700106

Näsi, M., Räsänen, P., Kaakinen, M., Keipi, T., & Oksanen, A. (2017). Do routine activities help predict young adults' online harassment: A multi-nation study. *Criminology & Criminal Justice*, *17*(4), 418–432. https://doi.org/10.1177/1748895816679865

National Incident-Based Reporting System. (2011). *National Incident-Based Reporting System: Using NIBRS data to understand victimization*. https://ovc.ojp.gov/sites/g/files/xyckuh226/files/pubs/NIBRS/pfv.html

Navarro, J. N., Clevenger, S., Beasley, M. E., & Jackson, L. K. (2017). One step forward, two steps back: Cyberbullying within social networking sites. *Security Journal*, *30*(3), 844–858. https://doi.org/10.1057/sj.2015.19

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773–793. https://doi.org/10.5281/zenodo.1234567

Ngo, F. T., Piquero, A. R., LaPrade, J., & Duong, B. (2020). Victimization in cyberspace: Is it how long we spend online, what we do online, or what we post online? *Criminal Justice Review*, *45*(4), 430–451. https://doi.org/10.1177/0734016820934175

Paradiso, M. N., Rollè, L., & Trombetta, T. (2024). Image-based sexual abuse associated factors: A systematic review. *Journal of Family Violence*, *39*(5), 931–954. https://doi.org/10.1007/s10896-023-00557-z

Pedersen, W., Bakken, A., Stefansen, K., & von Soest, T. (2022). Sexual victimization in the digital age: A population-based study of physical and image-based sexual abuse among adolescents. *Archives of Sexual Behavior*, *52*, 399–410. https://doi.org/10.1007/s10508-021-02200-8

Popp, A. M. (2012). The difficulty in measuring suitable targets when modeling victimization. *Violence & Victims*, *27*(5), 689–709. https://doi.org/10.1891/0886-6708.27.5.689

Powell, A., & Henry, N. (2017). *Sexual violence in a digital age*. Palgrave Macmillan.

Powell, A., & Henry, N. (2019). Technology-facilitated sexual violence victimization: Results from an online survey of Australian adults. *Journal of Interpersonal Violence*, *34*(17), 3637–3665. https://doi.org/10.1177/0886260516672055

Powell, A., Scott, A. J., Flynn, A., & McCook, S. (2022). A multi-country study of image-based sexual abuse: Extent, relational nature and correlates of victimization experiences. *The Journal of Sexual Aggression*, 1–16. https://doi.org/10.1080/13552600.2022.2119292

Powell, A., Scott, A. J., & Henry, N. (2020). Digital harassment and abuse: Experiences of sexuality and gender minority adults. *European Journal of Criminology*, *17*(2), 199–223. https://doi.org/10.1177/1477370818788006

Pratt, T. C., & Turanovic, J. J. (2016). Lifestyle and routine activity theories revisited: The importance of "risk" to the study of victimization. *Victims & Offenders*, *11*(3), 335–354. https://doi.org/10.1080/15564886.2015.1057351

Puente, S. M., & Hernández, I. N. (2022). Cyber victimization within the routine activity theory framework in the digital age. *Revista de Psicología*, *40*, 1–28. https://doi.org/10.18800/psico.202201.009

Räsänen, P., Hawdon, J., Holkeri, E., Keipi, T., Näsi, M., & Oksanen, A. (2016). Targets of online hate: Examining determinants of victimization among young Finnish Facebook users. *Violence & Victims*, *31*(4), 708–725. https://doi.org/10.1891/0886-6708.VV-D-14-00079

Reynald, D. M. (2011). Factors associated with the guardianship of places: Assessing the relative importance of the spatio-physical and sociodemographic contexts in generating opportunities for capable guardianship. *The Journal of Research in Crime and Delinquency*, *48*(1), 110–142. https://doi.org/10.1177/0022427810384138

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

Rollero, C., Teresi, M., & Pagliaro, S. (2023). The role of sexting on the perception of image-based sexual abuse. *Journal of Interpersonal Violence*, *38*(21–22), 11727–11744. https://doi.org/10.1177/08862605231188131

Ruvalcaba, Y., & Eaton, A. A. (2020). Nonconsensual pornography among U.S. adults: A sexual scripts framework on victimization, perpetration, and health correlates for women and men. *Psychology of Violence*, *10*(1), 68–78. https://doi.org/10.1037/vio0000233

Sampson, R. J., Eck, J. E., & Dunham, J. (2010). Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure. *Security Journal*, *23*(1), 37–51. https://doi.org/10.1057/sj.2009.17

Sampson, R. J., & Lauritsen, J. L. (1990). Deviant lifestyles, proximity to crime, and the offender-victim link in personal violence. *The Journal of Research in Crime and Delinquency*, *27* (2), 110–139. https://doi.org/10.1177/0022427890027002002

Schwartz, M. D., DeKeseredy, W. S., Tait, D., & Alvi, S. (2001). Male peer support and a feminist routine activities theory: Understanding sexual assault on the college campus. *Justice Quarterly*, *18* (3), 623–650. https://doi.org/10.1080/07418820100095041

Schwartz, M. D., & Pitts, V. L. (1995). Exploring a feminist routine activities approach to explaining sexual assault. *Justice Quarterly*, *12*(1), 9–32. https://doi.org/10.1080/07418829500092551

Shapiro, G. K., Tatar, O., Sutton, A., Fisher, W., Naz, A., Perez, S., & Rosberger, Z. (2017). Correlates of tinder use and risky sexual behaviors in young adults. *Cyberpsychology, Behavior and Social Networking*, *20*(12), 727–734. https://doi.org/10.1089/cyber.2017.0279

Sinko, L., Munro-Kramer, M., Conley, T., & Saint Arnault, D. (2021). Internalized messages: The role of sexual violence normalization on meaning-making after campus sexual violence. *Journal of Aggression, Maltreatment, & Trauma*, *30*(5), 565–585. https://doi.org/10.1080/10926771.2020.1796872

Snaychuk, L. A., & O'Neill, M. L. (2020). Technology-facilitated sexual violence: Prevalence, risk, and resiliency in undergraduate students. *Journal of Aggression, Maltreatment, & Trauma*, *29*(8), 984–999. https://doi.org/10.1080/10926771.2019.1710636

Stogner, J., Miller, J. M., Fisher, B. S., Stewart, E. A., & Schreck, C. J. (2014). Peer group delinquency and sexual victimization: Does popularity matter? *Women & Criminal Justice*, *24*(1), 62–82. https://doi.org/10.1080/08974454.2013.842520

Tabachnik, B. G., & Fidell, L. S. (2013). *Using multivariate statistics* (6th ed.). Pearson.

Tamarit-Sumalla, M., Malpica-Lander, C., & Fernández-Cruz, V. (2022). Co-occurrence of online and offline victimization: A latent class analysis in university students. *Social Sciences*, *11*(1), 1–16. https://doi.org/10.3390/socsci11010016

Vakhitova, Z. I., Alston-Knox, C. L., & Mawby, R. I. (2022). Online routine activities and self-guardianship against cyber abuse. *Victims & Offenders*, 1–23. https://doi.org/10.1080/15564886.2021.2022056

Vakhitova, Z. I., Alston-Knox, C. L., Reeves, E., & Mawby, R. I. (2021). Explaining victim impact from cyber abuse: An exploratory mixed methods analysis. *Deviant Behavior*, *43*(10), 1–20. https://doi.org/10.1080/01639625.2021.1921558

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

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*, *32*(2), 169–188. https://doi.org/10.1177/1043986215621379

Vale, M., Pereira, F., Spitzberg, B. H., & Matos, M. (2022). Cyber-harassment victimization of Portuguese adolescents: A lifestyle-routine activities theory approach. *Behavioral Sciences & the Law*, *40*(3), 604–618. https://doi.org/10.1002/bsl.2596

Walker, K., & Sleath, E. (2017). A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media. *Aggression and Violence Behavior*, *36*, 9–24. https://doi.org/10.1177/0886260519853414

Whitty, M. T. (2015). Anatomy of the online dating romance scam. *Security Journal*, *28*(4), 443–455. https://doi.org/10.1057/sj.2012.57

Wick, E. S., Nagoshi, C., Basham, R., Jordan, C., Kyoung Kim, Y., Phuong Nguyen, A., & Lehmann, P. (2017). Patterns of cyber harassment and perpetration among college students in the United States: A test of routine activities theory. *International Journal of Cyber Criminology*, *11*(1), 24–38. https://doi.org/10.5281/zenodo.495770

Wolfe, S. E., Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2016). Routine cell phone activity and exposure to sext messages: Extending the generality of routine activity theory and exploring the etiology of a risky teenage behavior. *Crime & Delinquency*, *62*(5), 614–644. https://doi.org/10.1177/00111128714541192

Yar, M. (2005). The novelty of cybercrime. *European Journal of Criminology*, *2*(4), 407–427. https://doi.org/10.1177/147737080556056

Zhang, L., Welte, J. W., & Wieczorek, W. F. (2001). Deviant lifestyle and crime victimization. *Journal of Criminal Justice*, *29*(2), 133–143. https://doi.org/10.1016/S0047-2352(00)00089-1