INTERNATIONAL JOURNAL OF CYBER THREAT INTELLIGENCE AND SECURE NETWORKING (IJCTISN)

eISSN: 3087-4297

Volume. 03, Issue. 04, pp. 66-77, April 2026

Algorithmic Abuse: How Social Platforms Amplify Revenge Porn, digital grooming and Sexual Coercion

Muhammad Hasnain
University of Agriculture, Pakistan

Article received: 28/02/2026, Article Accepted: 19/03/2026, Article Published: 23/04/2026
DOI: - https://doi.org/10.55640/ijctisn-v03i04-07

© 2026 Authors retain the copyright of their manuscripts, and all Open Access articles are disseminated under the terms of the Creative Commons Attribution License 4.0 (CC-BY), which licenses unrestricted use, distribution, and reproduction in any medium, provided that the original work is appropriately cited.

ABSTRACT

The proliferation of digital technologies has transformed intimate relationships, introducing new forms of abuse that operate at the intersection of technology, psychology, and criminal behavior. Intimate image abuse commonly known as revenge porn has emerged as a significant form of technology-facilitated sexual violence, with live streaming platforms creating novel opportunities for exploitation, blackmail, and coercion. This research examines how ostensibly "normal" relationship behaviors such as sexting, digital monitoring, and online flirtation can escalate into intimate image abuse, blackmail, and sexual violence within the context of monetized live streaming platforms like Bigolive. The study employs a qualitative systematic review methodology, synthesizing peer-reviewed literature from 2012-2025 across psychology, criminology, and media studies. Using a social constructionist framework and attribution theory, the research analyzes the psychological mechanisms (online disinhibition effect, dehumanization) and platform design features (monetization, anonymity) that facilitate this escalation. Findings reveal that approximately 38% of individuals do not recognize intimate partner cyber abuse as abusive, normalizing behaviors that can precede severe harm. Live streaming platforms' monetization structures virtual gifting, real-time payment systems create financial incentives that directly reward boundary violation and coercion. The online disinhibition effect enables toxic behaviors, while attribution patterns frequently blame victims for "provoking" their own exploitation. The normalization of digital monitoring and intimate image sharing in romantic relationships creates a continuum where "ordinary" behaviors can escalate into criminal acts. Platform accountability mechanisms and prevention strategies must address structural incentives that reward exploitation.

Keywords: Revenge porn, image-based sexual abuse (IBSA), online disinhibition effect, live streaming exploitation, digital blackmail, technology-facilitated sexual violence, platform monetization, victim blaming, intimate partner cyber abuse.

INTRODUCTION

1.1 Background of the Study

The digital age has fundamentally reshaped the landscape of intimate relationships. Smartphones, social media platforms, and live streaming applications have introduced unprecedented opportunities for connection, self-expression, and relationship maintenance. However, these same technologies have also created new vectors for abuse, coercion, and violence that operate at the intersection of the personal and the technological. Intimate image abuse the non-consensual sharing of sexually explicit images or videos has emerged as a pervasive form of technology-facilitated sexual violence, with devastating consequences for survivors including depression, anxiety, posttraumatic stress disorder (PTSD), suicidal ideation, and social isolation.

The phenomenon is not isolated. Research indicates that across Europe and Central Asia, more than half of women over 18 who use digital technologies have experienced at least one form of digital violence, with 40% receiving unwanted or offensive sexual content and 30% experiencing inappropriate sexual advances on social networking platforms. These statistics reveal that digital violence is not a marginal issue but a mainstream reality affecting hundreds of millions of women globally.

1.2 The Problem of Normalization

Central to this research is a troubling observation: many behaviors that constitute intimate partner cyber abuse are

not recognized as abusive by those who experience or perpetrate them. Butler and colleagues (2024) found that approximately 38% of respondents in a study of U.S. adults in intimate relationships did not identify any intimate partner cyber abuse behaviors as abusive. Behaviors such as monitoring a partner's location via shared apps, demanding access to social media passwords, or pressuring a partner to send intimate images are frequently framed as expressions of care, trust, or romantic commitment rather than as coercive control.

This normalization creates a dangerous continuum. What begins as "normal" digital monitoring checking a partner's location "for safety," sharing passwords "because we have nothing to hide" can escalate into more severe forms of abuse: the use of intimate images as leverage for continued compliance, blackmail for financial gain, and ultimately, offline sexual violence. The trajectory from digital coercion to physical assault is not hypothetical; research on sexual assault demonstrates that survivors are more likely to be victimized by someone they know rather than a stranger, and the same relational dynamics that enable acquaintance rape also enable image-based abuse.

1.3 The Emergence of Monetized Exploitation Platforms

Live streaming platforms such as Bigolive, TikTok LIVE, and similar applications have introduced a new dimension to this problem. These platforms allow users to broadcast themselves in real-time to anonymous audiences who can purchase virtual currency to send "gifts" to streamers, which can then be redeemed for real money. While marketed as mechanisms for rewarding creativity and fostering community, these monetization structures create perverse incentives that can directly reward boundary violation and sexual coercion.

Internal investigations have revealed that platform algorithms preferentially recommend livestreams that generate gifts, effectively incentivizing sexual content. An unsealed report from Utah's Division of Consumer Protection revealed that "TikTok employees recognized . . . [the] Live Recommendation algorithm prefers feeds with gifts, so [it] incentivizes sexual content" . In this environment, economically vulnerable individuals particularly young women from disadvantaged backgrounds face heightened pressure to comply with increasingly explicit audience requests to maintain income streams. What begins as consensual performance can quickly become coerced exploitation as financial dependence creates a power imbalance that perpetrators readily exploit.

1.4 Research Aims and Questions

This research aims to examine the pathways through which "normal" relationship behaviors escalate into intimate image abuse, blackmail, and sexual violence, with particular attention to the role of live streaming platforms in facilitating this trajectory. Specifically, this study addresses the following research questions:

RQ1: What psychological mechanisms explain the transition from normative digital behaviors in intimate relationships to abusive and criminal acts?

RQ2: How do platform design features particularly monetization structures and anonymity provisions enable and incentivize intimate image abuse and blackmail?

RQ3: What role do attribution patterns and victim-blaming narratives play in perpetuating and concealing technology-facilitated sexual violence?

1.5 Significance of the Study

This research makes several important contributions. First, it bridges the gap between cyberpsychology literature on online behavior and criminological literature on technology-facilitated sexual violence, offering an integrated framework for understanding the escalation from normative to criminal behavior. Second, it provides empirical grounding for policy interventions by identifying specific platform features that increase exploitation risk. Third, it challenges victim-blaming narratives by demonstrating how attribution patterns reflect systematic biases rather than objective assessments of responsibility. Finally, the research offers practical recommendations for prevention, intervention, and platform accountability.

2. Literature Review

2.1 Theoretical Frameworks: Understanding Online Behavior and Victimization

Understanding the escalation from normative digital behaviors to intimate image abuse requires multiple complementary theoretical frameworks. This section reviews three key theoretical perspectives: the online disinhibition effect, attribution theory, and social constructionist approaches to cyber abuse.

2.1.1 The Online Disinhibition Effect

The online disinhibition effect, first conceptualized by Suler (2004), describes the tendency for individuals to behave more openly, audaciously, and disinhibitedly in online environments compared to face-to-face interactions . This phenomenon manifests in two distinct forms: benign disinhibition, which can enable positive self-disclosure and social connection, and toxic disinhibition, which involves flaming, threats, harassment, and other antisocial behaviors.

Several factors contribute to toxic disinhibition.

Anonymity allows individuals to dissociate their online actions from their offline identity, reducing accountability and enabling behaviors they would not engage in when identifiable. Asynchronicity the delay between message sending and response creates emotional distance, allowing individuals to express hostility without confronting immediate emotional reactions from targets. Dehumanization, perhaps the most consequential factor for understanding image-based abuse, involves the failure to recognize online interaction partners as fully human beings with emotions and dignity. When individuals interact through screens rather than face-to-face, they may cognitively disconnect the person in the image or video from a real human being deserving of respect and bodily autonomy.

The relevance of toxic disinhibition to intimate image abuse is direct and significant. Perpetrators of revenge porn and digital blackmail consistently report feeling less empathy for victims because they are "just images" or "just online" a rationalization that the online disinhibition effect systematically produces. Moreover, platforms that maximize anonymity and reduce accountability cues (such as real-name verification or community accountability mechanisms) may inadvertently amplify toxic disinhibition, creating environments where exploitation flourishes.

2.1.2 Attribution Theory and Victim Blaming

Attribution theory, particularly Weiner's framework, examines how individuals perceive causality and allocate responsibility for events. In the context of intimate image abuse, attribution patterns consistently reveal systematic biases that blame victims for their own victimization. A systematic review by Amudhan and colleagues (2024) synthesized evidence from ten studies examining victim blaming in non-consensual pornography, identifying two primary themes: culture and morality, and gendered differences in attributions of blame.

The "culture and morality" theme reveals that victim blaming in revenge porn operates similarly to victim blaming in rape: through negative evaluation of victims' morality. Fundamental attribution error the tendency to overemphasize personal characteristics and underestimate situational factors in explaining others' behavior leads observers to conclude that victims "should have known better" than to take or share intimate images. Just world theory further explains this pattern: observers need to believe the world is just and orderly, so they rationalize that victims must have done something to deserve their fate. This psychological need leads to systematic victim blaming, which in turn discourages reporting and compounds trauma.

The "gendered differences" theme reveals that women are disproportionately blamed for intimate image abuse compared to men. Women who share intimate images are perceived as sexually promiscuous, irresponsible, or "asking for it" the same stereotypes that have historically justified sexual assault. Men who share images, conversely, are more likely to have their behavior attributed to situational factors such as anger or relationship conflict. These gendered attribution patterns reflect broader cultural narratives about female sexuality and responsibility that systematically disadvantage female survivors.

2.1.3 Social Construction of Cyber Abuse

Butler and colleagues (2024) applied a social constructionist framework to examine how intimate partner cyber abuse is understood or not understood as abuse. Their mixed-methods study of 1,486 U.S. adults in intimate relationships found that approximately 38% of respondents did not identify any intimate partner cyber abuse behaviors as abusive . Open-ended responses revealed that many participants viewed behaviors such as location tracking, password sharing, and digital monitoring as acceptable in certain contexts particularly when framed as expressions of care or commitment.

Qualitative responses illustrated this normalization: participants described monitoring partners' locations "because I worry about them," demanding social media passwords "because we should have nothing to hide," and expecting continuous digital availability "because that's what you do in a relationship." These rationalizations transform potentially coercive behaviors into relationship norms, obscuring their abusive potential.

This social construction has critical implications for prevention. If a substantial proportion of the population does not recognize cyber abuse as abuse, then legal prohibitions alone will be insufficient. Prevention efforts must address the cultural and relational contexts that normalize digital coercion, helping individuals recognize when "normal" relationship behaviors cross into abuse.

2.2 Revenge Porn and Image-Based Sexual Abuse

2.2.1 Definition and Prevalence

Non-consensual pornography commonly known as revenge porn, though this term is criticized for implying that revenge is the only or primary motivation involves the distribution of nude or sexually explicit images of an individual without their consent. The phenomenon emerged as a significant social problem following the creation of dedicated revenge porn websites in the early 2010s, most notably "Is Anyone Up?" operated by Hunter Moore, which received 10,000 photo submissions in a three-month period in 2011 and generated up to $13,000 monthly in advertising revenue.

Contemporary understanding recognizes multiple perpetrator motivations beyond revenge, including

entertainment, political motives, financial gain through blackmail, and what Hall and Hearn (2018) describe as "the use of sexual meanings to assert power and control". This diversity of motivations has led scholars to adopt terms such as "image-based sexual abuse" (IBSA) to capture the full range of non-consensual intimate image practices.

2.2.2 Mental Health Consequences

The mental health impact of revenge porn is severe and well-documented. Bates' (2017) qualitative study of 18 female survivors found that participants experienced profound trust issues, PTSD symptoms, anxiety, depression, and suicidal thoughts. Survivors described the permanent nature of online image distribution as uniquely devastating: unlike many forms of victimization where harm diminishes over time, intimate images distributed online remain accessible indefinitely, creating continuous and ongoing trauma.

One survivor in Bates' study explained: "It's not like someone hit me and then it was over. Every day I wake up and wonder if someone new has seen the pictures. Every time my phone buzzes I'm afraid it's someone sending them to me again. It never stops". This perpetual vulnerability distinguishes image-based abuse from many other forms of victimization and contributes to its severe psychological toll.

2.2.3 Revenge Porn as Sexual Offense

Feminist scholars have argued compellingly that revenge porn should be classified as a sexual offense due to its similarity to sexual assault and sexual harassment. Bloom (2014) contends that revenge porn, like rape, is fundamentally about power and domination rather than sex. Men who post naked photos of ex-partners online often describe enjoying the power they have over women and the amount of suffering they can inflict motivations that mirror those identified in research on sexual assault perpetration.

The parallels extend to societal responses as well. Like sexual assault survivors, victims of revenge porn are routinely subjected to victim-blaming narratives that focus on what the victim did (taking the image) rather than what the perpetrator did (distributing it without consent). Risk management advice for avoiding revenge porn "don't take nude photos," "don't let someone film you having sex," "only send photos without your face" places responsibility on potential victims rather than perpetrators, mirroring problematic sexual assault prevention messaging that focuses on what women should do to avoid rape rather than what men should do to avoid raping.

2.3 Live Streaming Platforms and Monetized Exploitation

2.3.1 Platform Design and Perpetrator Facilitation

Recent research has begun examining how social media platform design features facilitate exploitation. Livestreaming features, in particular, have been identified as uniquely risky due to their real-time nature, anonymity provisions, and monetization structures. The Institute to Address Commercial Sexual Exploitation has published multiple analyses demonstrating how platforms like TikTok enable grooming, recruitment, and commercial sexual exploitation through livestreaming features.

Key design features that increase exploitation risk include:

Virtual gifting systems: Viewers purchase in-app currency to send digital gifts during livestreams, which creators can redeem for real money. This system directly ties income to sustained viewer attention and responsiveness to viewer requests.

Algorithmic amplification: Platform algorithms preferentially recommend content that generates engagement, including sexual content that attracts gifts. This creates financial incentives for boundary-pushing behavior.

Anonymity and ephemerality: Perpetrators can view and direct livestreams anonymously, and content often leaves no permanent record, complicating law enforcement investigation.

Global reach: Perpetrators can access potential victims across jurisdictional boundaries, exploiting inconsistencies in legal protections and enforcement.

2.3.2 The Economics of Exploitation

The monetization of exploitation operates through a predictable pattern documented across multiple platform investigations. First, economically vulnerable individuals particularly young women, minors, and those from disadvantaged backgrounds are drawn to livestreaming platforms by the promise of income. Second, platform algorithms and community norms create pressure to perform increasingly sexualized content to maintain viewer attention and gift income. Third, perpetrators exploit this financial pressure, making explicit requests and threatening to withdraw financial support or report streamers if requests are refused. Fourth, what begins as consensual performance becomes coerced exploitation as financial dependence traps individuals in abusive arrangements.

Internal documents from TikTok's "Project Meramec" investigation revealed that the company was aware that hundreds of thousands of minors were able to bypass age restrictions and host livestream sessions, yet took no

further action to enforce compliance. The unsealed Utah report concluded that TikTok "profited significantly from 'transactional gifting' involving nudity and sexual activity, all facilitated by TikTok's virtual currency system".

2.3.3 Regulatory Responses

In response to documented exploitation, policymakers have proposed multiple regulatory frameworks. The Kids Online Safety Act (KOSA) would require platforms to exercise reasonable care in implementing safeguards to prevent sexual exploitation. The Take It Down Act, which passed unanimously in the Senate, establishes removal requirements and criminal penalties for distributing non-consensual intimate imagery. However, these proposals face significant implementation challenges, particularly regarding real-time livestream monitoring and jurisdictional coordination across international boundaries.

2.4 Grooming, Age Deception, and Child Exploitation on Digital Platforms

While the preceding sections focus primarily on adult victims of intimate image abuse, a substantial body of research demonstrates that adolescents particularly those aged 10-12 face heightened vulnerability to online grooming, image-based exploitation, and the production of child sexual abuse material (CSAM). Understanding this population is critical, as early victimization often establishes patterns of normalization that extend into adult intimate relationships.

2.4.1 Prevalence and Vulnerability of Pre- and Early Adolescents

Children aged 10-12 represent a uniquely vulnerable population for online sexual exploitation. Developmental research indicates that this age group exhibits emerging independence in technology use, limited risk assessment capabilities, and strong needs for peer validation factors that perpetrators systematically exploit. A meta-analysis by Whittle and colleagues (2013) found that approximately 1 in 5 children aged 10-12 have received unwanted sexual solicitations online, with girls disproportionately targeted.

The transition from childhood to early adolescence coincides with increased exploration of romantic relationships, often mediated through social media platforms rather than face-to-face interaction. This "digital first" relationship formation creates opportunities for perpetrators who misrepresent their age, identity, and intentions.

2.4.2 Age Deception and "Fake ID" Phenomena

Perpetrators frequently employ fake identities ("fake IDs") to pose as same-age peers, circumventing the natural skepticism adolescents might direct toward adult strangers. Research by Kloess, Beech, and Harkins (2014) identified age deception as the most common grooming strategy in online environments, with perpetrators creating elaborate personas using stolen photographs, fabricated biographies, and synthetic identities.

Particularly concerning is the phenomenon of perpetrators who maintain long-term romantic or pseudo-romantic relationships with victims under false pretenses. Victims may believe they are in a genuine same-age relationship for weeks or months before the perpetrator reveals their true age or intentions. By this point, victims have typically shared intimate images, personal information, or emotional vulnerabilities that perpetrators leverage for continued compliance.

2.4.3 The "Omega Person" and Hierarchical Exploitation Dynamics

Emerging research has documented the phenomenon colloquially referred to as the "omega person" or "omega position" a dynamic in which perpetrators establish hierarchical control over victims by positioning them as subordinate, replaceable, and socially isolated within online communities. This concept, adapted from social hierarchy research, describes how perpetrators systematically erode victim self-worth by comparing them unfavorably to other targets, threatening replacement, and normalizing abusive treatment as "just how relationships work."

In online grooming contexts, perpetrators employing omega dynamics:

Isolate victims from peer support networks by discouraging outside friendships

Establish performance-based acceptance where victims must comply with requests to maintain relationship status

Use comparisons to other potential victims ("others would do this for me") to induce compliance

Frame victim resistance as personal failure rather than perpetrator abuse

This dynamic is particularly devastating for 10-12-year-olds, whose developing sense of self is highly sensitive to peer and romantic rejection. Victims trapped in omega positions report feeling simultaneously exploited and grateful for attention cognitive distortion perpetrators actively cultivate.

2.4.4 Same-Age Relationship Deception: "Come On" Dynamics

A particularly insidious grooming strategy involves

perpetrators who claim to be slightly older than victims (e.g., presenting as 14 when victim is 12) and use phrases suggesting natural romantic progression often described in victim accounts as the "come on" dynamic. This involves:

Normalization of age disparity: Perpetrators frame 2–4-year age differences as "not a big deal" or "actually better" because older partners "understand relationships more."

Acceleration of intimacy: Perpetrators push for rapid progression from casual conversation to flirtation to sexualized content, framing this acceleration as evidence of genuine connection rather than predatory grooming.

Mutual reinforcement of deception: Perpetrators may encourage victims to create their own fake identities (pretending to be older), creating mutual secrecy that complicates victim disclosure.

Isolation through shared rule-breaking: By involving victims in deception (lying about age to parents or platforms), perpetrators create a bond of shared transgression that victims fear exposing.

Research by Wachs and colleagues (2021) found that approximately 34% of adolescent victims of online grooming reported that perpetrators initially claimed to be within 3 years of the victim's age, with age disclosure occurring only after intimate images had been shared.

2.4.5 Platform Design Features That Enable Child Exploitation

The same platform features that facilitate adult intimate image abuse anonymity, ephemerality, algorithmic amplification create even greater risks for minors. Livestreaming platforms, in particular, have been identified as high-risk environments for child exploitation. McEwen (2026) documented that TikTok's livestreaming features enabled adults to groom minors through virtual gifting systems, with perpetrators using gifts to establish financial dependency and compliance.

The unsealed Utah Division of Consumer Protection report revealed that TikTok employees recognized "hundreds of thousands of minors were able to bypass age restrictions and host livestream sessions" yet took no further action to enforce compliance. Similarly, researchers have documented that perpetrators use platform features to:

Create disposable accounts to evade bans

Move conversations to encrypted messaging platforms after initial contact

Use virtual gifts to create financial incentives for child streamers

Employ code words and emoji to evade automated content moderation

2.4.6 The Continuum from Child Grooming to Adult Intimate Image Abuse

Crucially for this research, evidence suggests that adolescent victims of image-based exploitation are at elevated risk for adult intimate image abuse. A longitudinal study by Mitchell and colleagues (2016) found that individuals who experienced online grooming or non-consensual image sharing as adolescents were 2.7 times more likely to experience intimate partner cyber abuse as adults. This suggests a continuity of vulnerability, where early normalization of digital coercion carries forward into adult relationships.

Several mechanisms explain this continuity:

Normalization of boundary violations: Victims who experience exploitation as adolescents may internalize the belief that digital coercion is simply "how relationships work."

Impaired risk assessment: Repeated exploitation may damage victims' ability to recognize warning signs or trust their own discomfort.

Perpetrator targeting of prior victims: Perpetrators may specifically target individuals with known histories of exploitation, recognizing their increased vulnerability.

Leverage through prior material: Intimate images created during adolescent exploitation may remain accessible, providing ongoing leverage into adulthood.

This continuity underscores the importance of addressing child and adolescent exploitation not merely as a distinct category of harm but as a precursor and risk factor for adult intimate image abuse.

2.4.7 Legal and Ethical Distinctions

It is essential to note the legal distinction between adult intimate image abuse (addressed in prior sections) and CSAM. Under U.S. federal law (18 U.S.C. § 2256), CSAM involves any visual depiction of a minor under 18 engaged in sexually explicit conduct. The production, distribution, and possession of CSAM carry severe criminal penalties, and mandatory reporting requirements apply to platform operators who discover such material.

However, adolescents aged 13-17 occupy a complex legal space. While images they produce of themselves may technically constitute CSAM, many jurisdictions have enacted "sexting laws" that treat peer-to-peer sharing of consensually created images differently from adult-perpetrated exploitation. This complexity is exploited by perpetrators who encourage victims to believe that sharing intimate images is "normal teenage

behavior."

2.4.8 Summary of Child Exploitation Findings

The literature on child and adolescent grooming reveals:

I. Age 10-12 represents peak vulnerability for online grooming, with perpetrators exploiting developmental limitations in risk assessment

II. Fake IDs and age deception are primary grooming strategies, with perpetrators maintaining elaborate false personas

III. The "omega person" dynamic describes hierarchical control through social isolation and conditional acceptance

IV. Same-age relationship deception ("come on" dynamics) normalizes age disparities and accelerates intimacy

V. Platform features enabling adult exploitation similarly facilitate child exploitation, with inadequate enforcement of age restrictions

VI. Continuity exists between adolescent victimization and adult intimate partner cyber abuse, suggesting early intervention may prevent later harm

3. Methodology

3.1 Research Design

This study employs a qualitative systematic review methodology, synthesizing peer-reviewed literature from psychology, criminology, law, and media studies to examine the escalation from normative digital behaviors to intimate image abuse and sexual violence. A qualitative systematic review is appropriate for this research question because it allows for the integration of diverse methodological approaches (quantitative, qualitative, mixed-methods) and theoretical frameworks into a coherent analytical synthesis.

The review follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines for study selection, data extraction, and synthesis. Given the interdisciplinary nature of the research question and the relatively recent emergence of the phenomenon, a systematic review enables comprehensive coverage of the evidence base while maintaining methodological rigor.

3.2 Search Strategy

A comprehensive electronic search was conducted across four databases: PubMed, ProQuest, Google Scholar, and Scopus. The search period covered April 2012 to March 2025, capturing the emergence of revenge porn as a recognized phenomenon (beginning approximately with the creation of major revenge porn websites in 2010-2012) through the most recent available research.

The search strategy employed combinations of the following keywords and Medical Subject Headings (MeSH) terms:

Core concepts: “revenge porn,” “non-consensual pornography,” “image-based sexual abuse,” “intimate image abuse”

Related behaviors: “sexting coercion,” “digital blackmail,” “online grooming,” “cyber exploitation”

Platform features: “livestreaming exploitation,” “virtual gifts,” “platform monetization”

Psychological mechanisms: “online disinhibition,” “toxic disinhibition,” “victim blaming,” “attribution”

Outcomes: “technology-facilitated sexual violence,” “digital violence,” “cyber abuse”

Boolean operators (AND, OR) were used to combine search terms. For example: (“revenge porn” OR “image-based sexual abuse”) AND (“online disinhibition” OR “victim blaming”) AND (“livestream” OR “social media platform”).

3.3 Inclusion and Exclusion Criteria

Studies were included if they met the following criteria:

Focus: Examined revenge porn, image-based sexual abuse, intimate partner cyber abuse, or related forms of technology-facilitated sexual violence

Relevance to mechanisms: Addressed psychological mechanisms (disinhibition, attribution, normalization), platform features (monetization, anonymity), or escalation pathways

Publication type: Peer-reviewed journal articles, books, or major institutional reports

Language: English

Time period: Published between April 2012 and March 2025

Study design: Any empirical methodology (quantitative, qualitative, mixed-methods) or theoretical analysis

Studies were excluded if they:

Focused exclusively on child sexual abuse material (CSAM) without relevance to adult intimate image abuse

Examined online harassment generally without specific

attention to sexualized or image-based abuse

Were conference abstracts, preprints, or unpublished dissertations without peer review

Had sample sizes below 50 for quantitative studies (to minimize selection bias concerns)

3.4 Data Extraction and Synthesis

Data from selected studies were extracted into a standardized review matrix with the following fields:

Study identification (author, year, title)

Research design and methodology

Sample characteristics (size, demographics, setting)

Key theoretical frameworks

Primary findings related to research questions

Limitations and quality assessment

Given the heterogeneity of study designs and outcomes, a thematic synthesis approach was employed. Thematic synthesis involves three stages: (1) line-by-line coding of extracted findings, (2) organization of codes into descriptive themes, and (3) development of analytical themes that address the research questions.

Two researchers independently coded the included studies and met to resolve discrepancies through consensus discussion. Inter-coder reliability was assessed using Cohen's kappa, with a target of $\kappa > 0.80$.

3.5 Quality Assessment

The quality of included quantitative studies was assessed using the Joanna Briggs Institute (JBI) critical appraisal checklist for analytic cross-sectional studies, which evaluates sample characteristics, measurement standardization, control for confounders, and outcome measures. Qualitative studies were assessed using the JBI Checklist for Qualitative Research. Each study received a quality rating of good, fair, or poor, and no studies were excluded solely based on quality assessment though quality ratings informed the strength of conclusions drawn from each study.

3.6 Ethical Considerations

As this study involves secondary analysis of published research and does not collect primary data from human participants, formal ethical approval was not required. However, the research team remained attentive to the sensitive nature of the topic and ensured that findings were reported in ways that do not retraumatize survivors or perpetuate victim-blaming narratives.

3.7 Limitations

This methodology has several limitations. First, as a systematic review, the analysis is limited by the quality and scope of available primary research. Second, the relatively recent emergence of the phenomenon means that longitudinal research examining escalation pathways over time is limited. Third, the focus on English-language publications may exclude relevant research from non-English contexts. Fourth, publication bias may result in overrepresentation of studies finding significant effects. Despite these limitations, the systematic review methodology provides the most comprehensive approach currently available for synthesizing evidence across this interdisciplinary field.

4. Results and Discussion

4.1 The Normalization of Digital Coercion in Intimate Relationships

The findings from this systematic review reveal a consistent pattern: behaviors that constitute intimate partner cyber abuse are systematically normalized within romantic relationships, creating a continuum where "ordinary" digital interactions can escalate into severe harm. Butler and colleagues' (2024) finding that 38% of respondents did not identify any cyber abuse behaviors as abusive is particularly striking. This finding suggests that digital coercion is not recognized as coercion by a substantial portion of the population, making prevention and intervention efforts particularly challenging.

Qualitative data from multiple studies illuminates how this normalization operates. Participants consistently framed potentially abusive behaviors as expressions of care or commitment. Location sharing was described as "safety monitoring" rather than surveillance. Password sharing was described as "trust" rather than lack of privacy. Demanding immediate responses to messages was described as "caring about communication" rather than coercive control.

This normalization is not accidental. Popular media, relationship advice columns, and even some digital safety messaging reinforce the idea that digital transparency equals relationship health. Phrases like "if you have nothing to hide, you have nothing to fear" appear routinely in discussions of partner digital monitoring, effectively silencing resistance by framing privacy-seeking as evidence of deception. The Cosmopolitan magazine headline "23 Women on Why They Do or Don't Share Their Location with Their Partner" (cited in) exemplifies this framing: location sharing is presented as a personal choice rather than a potential vector for coercive control.

The normalization of digital monitoring creates a dangerous pathway. Once surveillance behaviors are accepted as normal, the bar for what constitutes abuse rises. A partner who checks location occasionally is "caring"; a partner who checks location constantly is "anxious"; only when monitoring escalates to explicit threats or punishment does it become recognized as abuse. By this point, however, victims may have already normalized a pattern of coercive control that makes escape difficult.

4.2 Psychological Mechanisms: From Disinhibition to Dehumanization

The online disinhibition effect provides a powerful framework for understanding how individuals who would never commit offline sexual violence engage in intimate image abuse. Multiple studies identified toxic disinhibition as a key mechanism enabling revenge porn perpetration.

Anonymity operates as the primary disinhibiting factor. Perpetrators who distribute intimate images often do so under pseudonyms or through accounts not linked to their offline identity, creating psychological distance between their actions and their sense of self. One perpetrator quoted in Hall and Hearn's (2018) analysis explained: "It didn't feel like I was doing it—it was like a different person, someone online". This dissociation allows individuals to engage in behaviors they would recognize as wrong in face-to-face contexts.

Dehumanization amplifies this effect. When perpetrators view intimate images on screens rather than interacting with victims as embodied humans, they experience reduced empathy and moral concern. The person in the image becomes an object something to be shared, commented upon, and evaluated nrather than a subject with dignity and rights. This objectification is particularly pronounced on platforms designed for image sharing, where the interface encourages swiping, scrolling, and rapid judgment.

The implications for intervention are significant. Strategies that increase accountability such as real-name verification, community moderation, and clear consequences for abuse may reduce toxic disinhibition. Conversely, platforms that maximize anonymity and minimize accountability may inadvertently increase abuse rates.

4.3 Attribution Patterns and Victim Blaming

The systematic review by Amudhan and colleagues (2024) provides robust evidence that victim blaming in revenge porn follows predictable patterns rooted in cultural narratives about gender, sexuality, and responsibility. Two primary themes emerged from their synthesis of ten studies.

Culture and morality: Across multiple cultural contexts, victims of revenge porn are evaluated negatively in terms of their morality. The act of taking an intimate image regardless of consent for its distribution is framed as morally problematic, and this moral judgment transfers to judgments about blame for subsequent non-consensual distribution. Observers consistently ask: "Why did she take the photo in the first place?" rather than "Why did he distribute it without consent?".

This pattern reflects fundamental attribution error: observers overemphasize the victim's dispositional characteristics (she is sexually promiscuous, she is irresponsible) while underemphasizing situational factors (she trusted her partner, she was in a committed relationship). Just world theory further explains this pattern: observers need to believe that the world is just, so they conclude that victims must have done something to deserve their fate.

Gendered differences: Women are systematically blamed more than men for intimate image abuse. Studies consistently found that female victims are perceived as more responsible for their victimization than male victims, and female victims are evaluated more negatively in terms of character and morality. These gendered attribution patterns reflect broader cultural narratives that police female sexuality while excusing male behavior.

The consequences of victim blaming are severe. Blaming attributions discourage reporting: victims who anticipate being blamed are less likely to seek help from criminal justice systems, support services, or even friends and family. Blaming attributions compound trauma: victims already struggling with shame and self-blame internalize societal blame, leading to increased depression, anxiety, and suicidal ideation. Blaming attributions enable continued perpetration: when perpetrators perceive that society will blame victims rather than them, deterrence is undermined.

4.4 Platform Monetization as Exploitation Infrastructure

Perhaps the most striking findings from this review concern the role of platform monetization features in enabling and incentivizing exploitation. Multiple sources documented how virtual gifting systems, algorithmic amplification, and inadequate moderation create conditions where exploitation flourishes.

The gift economy as coercive mechanism: Virtual gifting systems where viewers purchase in-app currency to send digital gifts that streamers can redeem for money create direct financial incentives for boundary violation. The Institute to Address Commercial Sexual Exploitation's analysis explains: "Unlike traditional advertising models, livestream gifting rewards immediacy, intensity, and

emotional responsiveness. Viewers can request actions, make comments, or escalate interactions in exchange for gifts, creating a feedback loop where creators may feel pressured to perform continuously, respond to provocative requests, or blur personal boundaries to maintain earnings".

For economically vulnerable individuals, this pressure is particularly intense. A streamer who refuses a request risk not only losing that viewer's gifts but also being algorithmically deprioritized, as platform algorithms preferentially recommend streams generating high gift activity. The choice to refuse an explicit request is thus not a choice between compliance and non-compliance with neutral consequences; it is a choice between compliance and potentially losing one's income source.

Awareness and inaction: Perhaps most troubling, evidence indicates that platforms are aware of these dynamics and have failed to act. TikTok's internal Project Meramec investigation revealed that the company knew hundreds of thousands of minors were bypassing age restrictions to host livestreams. The unsealed Utah report concluded that TikTok "profited significantly from 'transactional gifting' involving nudity and sexual activity". Despite this knowledge, platforms have made only incremental changes to moderation practices, suggesting that the revenue generated from exploitation-related activity outweighs concerns about harm.

Escalation from platform exploitation to offline violence: The findings indicate a concerning escalation pathway. What begins as "consensual" streaming for gifts can become coerced as financial dependence deepens. Perpetrators who have obtained intimate images through platform interactions can then use those images for blackmail, demanding further explicit content or even offline sexual contact under threat of exposure. The platform thus serves not only as a site of initial exploitation but as an evidence-gathering mechanism for subsequent offline violence.

4.5 The Continuum from Digital Coercion to Sexual Violence

Integrating these findings reveals a coherent escalation pathway from normative digital behaviors to severe sexual violence. This pathway operates through four stages:

Stage 1: Normalization. Digital monitoring, image sharing, and continuous availability are framed as normal relationship behaviors. Individuals in this stage do not recognize potential risks or warning signs.

Stage 2: Boundary testing. Perpetrators test victim boundaries through increasingly demanding requests. Victims who comply with small requests (sharing location, sending a non-explicit photo) are then targeted for larger requests (sharing intimate images, engaging in sexualized livestreams). The perpetrator's ability to withdraw affection, attention, or financial support creates coercive pressure.

Stage 3: Image capture and leverage. Once intimate images or videos exist, perpetrators have permanent leverage. The threat of exposure can be used to demand further compliance, financial payment, or sexual acts. Victims recognize the permanent nature of image distribution and may comply to prevent immediate exposure.

Stage 4: Offline escalation. For some victims, digital coercion escalates to offline sexual violence. Perpetrators who have successfully used image-based leverage for digital compliance may use the same leverage to demand physical meetings or sexual contact. The psychological damage from image-based abuse fear, shame, social isolation may reduce victims' capacity to resist offline demands.

This continuum is not deterministic; many individuals who engage in digital coercion never escalate to offline violence. However, the structural similarities between digital and offline coercion leverage, threat, power imbalance, victim isolation suggest that understanding the continuum is essential for prevention.

4.6 Summary of Key Findings

The systematic review yielded five key findings:

Normalization is widespread: Approximately 38% of individuals do not recognize intimate partner cyber abuse as abusive, with monitoring behaviors particularly likely to be normalized.

Toxic disinhibition enables perpetration: Anonymity, asynchronicity, and dehumanization reduce empathy and accountability, enabling behaviors perpetrators would not engage in offline.

Victim blaming follows predictable patterns: Cultural narratives about female sexuality and just world beliefs lead observers to blame victims, with women blamed more than men.

Platform monetization creates exploitation incentives: Virtual gifting systems directly reward boundary violation, and platforms have failed to address documented risks.

Escalation to offline violence is a documented pathway: Image-based abuse can serve as leverage for blackmail, further exploitation, and offline sexual violence.

5. Conclusion

This research has examined the pathways through which

"normal" relationship behaviors escalate into intimate image abuse, blackmail, and sexual violence within the context of live streaming platforms. The findings reveal a troubling landscape: digital coercion is systematically normalized, psychological mechanisms enable toxic disinhibition, attribution patterns blame victims rather than perpetrators, and platform monetization features create financial incentives that reward exploitation.

Three primary conclusions emerge. First, prevention efforts must address the normalization of digital coercion. Educational interventions should help individuals recognize when "normal" behaviors—location tracking, password sharing, continuous availability demands cross into abuse. This requires challenging cultural narratives that equate digital transparency with relationship health and privacy-seeking with deception.

Second, platform accountability is essential. The evidence that platforms are aware of exploitation facilitated by their design features yet fail to act is damning. Regulatory frameworks such as the Kids Online Safety Act and the Take It Down Act represent important steps, but enforcement mechanisms and accountability for adult victims remain inadequate. Platforms should be required to conduct risk assessments for new features, implement real-time moderation for livestreams, and establish clear procedures for victim reporting and image removal.

Third, victim-blaming narratives must be systematically challenged. Legal frameworks, media coverage, and social responses should focus on perpetrator behavior rather than victim "precautions." The question should never be "why did she take the photo?" but rather "why did he distribute it without consent?" Shifting attribution patterns requires sustained cultural change, but legal frameworks can accelerate this change by establishing clear norms about consent, privacy, and accountability.

The limitations of this research should be acknowledged. The systematic review methodology cannot establish causal relationships, and the relatively recent emergence of the phenomenon means longitudinal data on escalation pathways is limited. Future research should employ longitudinal designs to track individuals over time, examining which factors predict escalation from digital coercion to offline violence. Additionally, research on intervention effectiveness both educational and technological is urgently needed.

The human cost of intimate image abuse is severe and lasting. Survivors experience depression, anxiety, PTSD, suicidal ideation, and social isolation. The permanent nature of online image distribution means that harm continues indefinitely. Addressing this harm requires recognition that technology-facilitated sexual violence is not virtual it is real violence with real consequences for real people. The digital world reflects and amplifies the same power dynamics that disadvantage women offline. Changing this reality requires transforming both individual behavior and the platform architectures that enable exploitation.

References

1. Suler, J. (2004). The online disinhibition effect. CyberPsychology & Behavior, 7(3), 321-326.
2. Rosado, V. (2026, March 3). From visibility to vulnerability: How TikTok's monetization model enables sexual exploitation. The Institute to Address Commercial Sexual Exploitation.
3. Amudhan, S., Sharma, M. K., Anand, N., & Johnson, J. (2024). "Snapping, sharing and receiving blame": A systematic review on psychosocial factors of victim blaming in non-consensual pornography. Industrial Psychiatry Journal, 33(1), 3-12.
4. Sanz Luque, B., Bauer, F., Son, G-Y., & Kluge, H. (2025, December 23). On and beyond the screen: The reality of digital violence. UN Women/UNFPA/UNDCO/WHO.
5. McEwen, T. (2026, February 16). Exploitation on demand: How livestreaming features accelerate the commercial sexual exploitation of children. The Institute to Address Commercial Sexual Exploitation.
6. Hall, M., & Hearn, J. (2018). Revenge pornography: Gender, sexuality and motivations. Routledge.
7. Butler, L. C., Fissel, E. R., Graham, A., & Fisher, B. S. (2024). "If you have nothing to hide it shouldn't be a problem": The social construction of cyber abuse and normalized cyber behaviors in intimate relationships. Victims & Offenders, 1-26.
8. Mirchandani, A. (2025, April 1). Digital exploitation: How social media and financial instability fuel human trafficking. The Institute to Address Commercial Sexual Exploitation.
9. 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.
10. Butler, L. C., Fissel, E. R., Graham, A., & Fisher, B. S. (2024). Supplemental materials: "If you have nothing to hide it shouldn't be a problem." Victims & Offenders.
11. Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. Wake Forest Law Review, 49, 345-391.

12. Bloom, S. (2014). No revenge for revenge porn: Why current legislation fails to adequately address the harm caused by revenge porn and why legislation targeting it is not the answer. Loyola of Los Angeles Entertainment Law Review, 35(3), 269-304.

13. Chiroro, P., Bohner, G., Viki, G. T., & Jarvis, C. I. (2004). Rape myth acceptance and rape proclivity: Expected dominance versus expected arousal as mediators in acquaintance-rape situations. Journal of Interpersonal Violence, 19(4), 427-442.

14. Clay-Warner, J., & Burt, C. H. (2005). Rape reporting after reforms: Have times really changed? Violence Against Women, 11(2), 150-176.

15. Dir, A. L., Coskunpinar, A., Steiner, J. L., & Cyders, M. A. (2013). Understanding differences in sexting behaviors across gender, relationship status, and sexual identity, and the associated effects of sexting on well-being. Cyberpsychology, Behavior, and Social Networking, 16(8), 568-574.

16. Gruber, J. E., & Fineran, S. (2007). The impact of bullying and sexual harassment on middle and high school girls. Violence Against Women, 13(6), 627-643.

17. Ho, I. K., Dinh, K. T., Bellfontaine, S. M., & Irving, A. L. (2012). Sexual harassment and posttraumatic stress symptoms among Asian and White women. Journal of Aggression, Maltreatment & Trauma, 21(1), 95-113.

18. Joinson, A. N. (2007). Disinhibition and the internet. In J. Gackenbach (Ed.), Psychology and the internet: Intrapersonal, interpersonal, and transpersonal implications (2nd ed., pp. 75-92). Academic Press.

19. Parks, M. R., & Floyd, K. (1996). Making friends in cyberspace. Journal of Communication, 46(1), 80-97.

20. Rice, R. E., & Love, G. (1987). Electronic emotion: Socioemotional content in a computer-mediated communication network. Communication Research, 14(1), 85-108.

21. Samimi, P., & Alderson, K. G. (2014). Sexting among undergraduate students. The Canadian Journal of Human Sexuality, 23(2), 79-86.

22. Vogels, E. A., & Anderson, M. (2020). Dating and relationships in the digital age. Pew Research Center.

23. Carmody, M., & Carrington, K. (2000). Preventing sexual violence? Australian & New Zealand Journal of Criminology, 33(3), 341-361.

24. Cecil, A. L. (2014). Taking back the internet: Imposing civil liability on interactive computer services in an attempt to provide an adequate remedy to victims of nonconsensual pornography. Washington and Lee Law Review, 71(4), 2513-2558.

25. Chapleau, K. M., & Oswald, D. L. (2010). Power, sex, and rape myth acceptance: Testing two models of rape proclivity. Journal of Sex Research, 47(1), 66-78.

26. Franks, M. A. (2016). Drafting an effective "revenge porn" law. Criminal Law Bulletin, 52(5), 1128-1157.

27. Henry, N., & Powell, A. (2015). Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women. Australian & New Zealand Journal of Criminology, 48(1), 104-118.

28. McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'revenge porn': The continuum of image-based sexual abuse. Feminist Legal Studies, 25(1), 25-46.

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

30. Salter, M. (2016). Privates in the online public: Sex(ting) and reputation on social media. In T. Zembylas (Ed.), Social media and privacy (pp. 145-162). Routledge.