A Model of IBSA Harm Reduction: Image Angel's Proposed Impact on Perpetrator Behaviour

By Dr. Josie West

About Image Angel

Image Angel is a cutting-edge deterrence tool designed to combat image-based abuse. It works by embedding invisible and non removable watermarks into every live broadcast, image and frame of video downloaded from supported platforms. Each watermark links the image to its specific recipient. If the content is later shared without consent, the watermark provides undeniable proof of who was responsible, removing deniability and shifting accountability onto the perpetrator. Developed in direct response to the rise in intimate image offences, Image Angel empowers victims with forensic evidence. It deters abuse by eliminating anonymity and supports safer digital environments, enhancing safety without sacrificing privacy.

About STISA

Survivors & Tech Solving Image-Based Sexual Abuse (STISA) is a pioneering global initiative, founded in 2024, that places victims and survivors at the heart of its mission to address Image-Based Sexual Abuse (IBSA). We unite and strengthen helplines, hotlines, and other survivor-support initiatives worldwide, working to ensure the prompt removal of abusive online content that infringes on personal intimacy. STISA envisions a world where every victim and survivor of IBSA is empowered, respected, and supported, fostering a global community committed to protecting their dignity, amplifying their voices, and upholding their rights.

Table of **Contents**

Methodology

This whitepaper combines a thematic literature review with insights from primary data collection via stakeholder polling. The research design focused on examining both existing academic frameworks and lived experiences related to image-based sexual abuse (IBSA), with the aim of informing a harm-reduction model grounded in technology, behavioural intervention and survivor advocacy.

Literature Review

A thematic literature review was conducted to contextualise the model of harm reduction proposed in this whitepaper. The review focused on four key domains:

1. Image-Based Sexual Abuse: Empirical studies and legal frameworks were analysed to map the impact, typologies, motivations and technological vectors of IBSA perpetration.

2. Perpetrator Behaviour: Behavioural psychology, criminological profiles and interventions for digital sexual offences were explored to understand drivers of harm and models of harm reduction.

3. Accountability Mechanisms: Literature was examined on platform governance and accountability, legal frameworks and institutional actors in preventing and responding to IBSA.

4. Gender-Based Violence (GBV) Reduction Models: Broader literature on GBV was reviewed, alongside research on legal, informal and restorative justice approaches. This included both carceral and non-carceral responses to IBSA, aiming to situate the issue within gendered power structures.

Searches were conducted using the academic database Google Scholar, alongside Google search for great literature searchers, with inclusion criteria focused on peer-reviewed articles and subject-specific reports. Priority was given to perpetrator and survivor-informed analyses.

The review followed an integrative and human-centred thematic strategy, drawing from methods outlined by Kulczak-Dawkins et al., (2018). This approach used a long-range lens to incorporate diverse disciplinary perspectives, particularly from social sciences, criminology, legal and behavioural studies, to identify underlying factors in decision-making and harm perpetuation. By doing so, it supported a conceptual reframing of IBSA not only as a legal or moral issue, but as one shaped by complex social-psychological processes.

Additionally, the six-phase thematic analysis method of Braun and Clarke, as applied by Horntvedt et al. (2018), informed the data synthesis. Initial codes were developed deductively based on the review's guiding questions, allowing for the emergence of key themes. Findings were iteratively reviewed and refined to ensure conceptual coherence and relevance to harm reduction modelling. The guiding questions that informed the coding process were: What is the scope and harm of image-based sexual abuse? What are the motivators and predictors of this behaviour? And what interventions might effectively change perpetrator behaviour?

Survey Methodology

In the section titled 'The Scope and Harm of Intimate Image Abuse,' findings from a poll obtained for a previous whitepaper were included. Primary insights were gathered through a live poll organised and hosted by adult industry consultants Thornhill Digital on behalf of Image Angel, in April 2025. The webinars, attended primarily by online sex workers, focused on digital safety and platform accountability. Attendees were invited to participate in a series of poll questions addressing their perceptions of image-based abuse, platform accountability and attitudes towards safety. The webinar hosted 60 online sex workers, 40 of which participated in the polls.

Participation was voluntary and responses were collected in real time using a secure polling tool embedded in the webinar platform. While the sample is not statistically representative, it offers critical experiential data from communities disproportionately impacted by IBSA and underrepresented in formal studies. Responses were thematically coded for our whitepaper, 'UK Sex Workers' Perceptions of Image Based Sexual Abuse Protections on Digital Platforms,' which enabled identification of patterns relevant to this whitepaper.

Introduction

On a Sunday morning in August 2020, reality TV star Georgia Harrison crossed the street to have a cup of tea with her neighbour, fellow influencer Stephen Bear (Moore, 2023). They had a shared history in the limelight and a complicated romantic past. What unfolded that day would change her life entirely. Without her knowledge or consent, Bear filmed them having sex in his garden on CCTV. Months later, the footage was uploaded to his OnlyFans and rapidly spread across the internet, including on Pornhub. Harrison found out when she received a screenshot from a fan in the US. Instead of retreating, she reported the crime, waived her right to anonymity and took her case to court.

In March 2023, Bear was sentenced to 21 months in prison for voyeurism and the non-consensual sharing of intimate images (Moore, 2023). Harrison's decision to speak out sparked national attention, triggered a 56% rise in calls to the UK's revenge porn helpline and helped secure legislative changes to better protect victims (ibid). Her story offered a rare victory in a landscape where prosecutions are rare, and justice is even rarer. Yet, as this paper shows, Georgia Harrison's case is far from isolated – and most victims don't have the same platform or legal success. Bringing perpetrators to court is not the typical experience, especially in the adult sector, where sex workers are disproportionately targeted and often silenced by stigma, platform inaction and legal ambiguity. This whitepaper draws into focus how platforms can aid in holding perpetrators accountable

The digital era has transformed how people communicate, express themselves and engage in intimate relationships. However, new forms of harm have also emerged. Image based-sexual abuse (IBSA) refers to the non-consensual creation, distribution, or threat of distribution of intimate or sexual images of another person. This conduct includes recording sexual acts without consent, sharing "revenge porn," and distributing images for financial exploitation or humiliation. According to McGlynn et al. (2017), the term encompasses; 1) Image-based sexual

abuse: any sharing or threat to share sexual images without consent; 2) Upskirting: surreptitious photography under clothing; 3) Deepfakes: synthetic sexual imagery created with AI; 4) Sexual extortion ("sextortion"): threats to release intimate images unless demands are met.

While IBSA affects a wide range of individuals, those in the adult entertainment industry often experience a heightened level of risk due to the nature of their work and the environments in which they operate. Concerns include content theft, privacy breaches, reputational harm and economic disruption. Despite growing public awareness, many structural and legal gaps remain, and platform responses are often limited or inconsistent.

This white paper explores the scope, consequences, and drivers of intimate image abuse, with particular attention to the experiences of sex workers. It also discusses how *Image Angel* is a technology-led solution designed to mitigate and prevent these harms through evidence capture. This is essential to shaping the conversation around changing perpetrator behaviour—both by addressing the motivations behind such offences and by strengthening the consequences for these acts of violence. Drawing upon a robust body of academic research, we argue that IBSA is a gendered, socially sanctioned form of violence facilitated by historic gaps in platform accountability, weak legal frameworks and cultural tolerance for violent behaviour online.

Executive **Summary**

The first part of this white paper explores the scope and impact of IBSA, drawing on academic research. Victims frequently report severe psychological, social and economic harms, including anxiety, depression, isolation and career disruption. Within the sex industry, image abuse is often perpetrated by clients or others with access to private content, with consequences ranging from outing and reputational damage to blackmail and loss of livelihood.

Gaps in preventative technologies and reporting systems on platforms contribute to the persistence of IBSA. These include weak identity checks, slow takedown processes, an over-reliance on victims to self-report violations and a generalised belief among perpetrators that it's not a significant crime. The legal framework also remains limited, with challenges in proving intent, enforcing cross-border claims and ensuring protection for sex workers, who may be reluctant to engage with authorities due to stigma or fear of criminalisation. The combination of legal ambiguity, systemic negligence and cultural acceptance of coercive image sharing continues to leave many victims without adequate recourse.

In response to this landscape, the final section of the paper introduces *Image Angel*—a multi-layered technological intervention aimed at deterring and documenting IBSA. Forensic watermarking[1] embeds invisible, traceable user-level data into each image at the point of access, creating a record of who viewed what and when. Digital fingerprinting (hashing)[2] can then be used to detect whether that same content appears elsewhere. This creates a record of who viewed what, when — and enables platforms to identify the source if that content is leaked. Image Angel enhances the traceability of content and raises the perceived risk of offending. In doing so, it

---

[1] Forensic watermarking embeds invisible, traceable markers into digital content, allowing identification of the source platform even if the content is copied, altered, or scraped.

[2] Hashing is a method that creates a unique digital fingerprint of content, allowing platforms to detect identical material elsewhere and trace access in case of leaks.

targets key drivers of abuse, including the sense of anonymity and impunity often felt by perpetrators.

In addition to technological solutions, Image Angel proposes a framework for early intervention and public education. This includes mandatory consent training, user-focused platform integrations and workshops challenging harmful myths about image sharing. While technology alone cannot address all forms of abuse—particularly those rooted in sadistic or controlling behaviours—it can make IBSA more difficult to perpetrate and less socially permissible.

The paper concludes that technology must work in tandem with informed policy development, platform accountability and survivor-led advocacy. A proactive, prevention-focused and layered holistic approach—rather than a solely punitive one—offers the greatest potential to reduce the prevalence of intimate image abuse and to protect those most vulnerable to its harms.

The Scope and Harm of Intimate Image Abuse

The literature consistently describes Image-Based Sexual Abuse (IBSA) as a broad spectrum of behaviours, situated on the continuum of sexual violence and facilitated by pervasive digital technologies (McGlynn et al., 2017). It is increasingly recognised as a gendered form of abuse that replicates patterns of control and coercion commonly seen in intimate partner violence (Eaton et al., 2021). These behaviours cause profound psychological harm, including anxiety, depression, social withdrawal and loss of livelihood (Paradiso et al., 2024). For those in the adult entertainment industry, where IBSA occurs more frequently than in the general population, the threat can be weaponised to exert control, extract money, compromise anonymity or cause reputational damage (West, 2024).

According to Paradiso et al., (2024) victims report wide-ranging psychological, social and economic damage. This includes specific harms related to mental health such as *anxiety* (Short et al., 2017; Bates, 2017; Campbell et al., 2020; Champion et al., 2022), *depression* (Bates, 2017; Aborisade, 2021; Champion et al., 2022), *post-traumatic stress disorder* (Bates, 2017), *stress*, *anger*, *sleep disorders* and *substance misuse* (Bates, 2017; Short et al., 2017; Aborisade, 2021; Champion et al., 2022), alongside *self-harm*, *suicide attempts* and *suicidal ideation* (Bates, 2017; Short et al., 2017; Aborisade, 2021; Champion et al., 2022).

Victims experienced profound loss of control over their bodies and images (Bates, 2017; Champion et al., 2022). Many became hyper-vigilant, monitoring websites and closing social media accounts (Aborisade, 2021; McGlynn et al., 2021). Significant declines in self-confidence and self-esteem were reported (Bates, 2017). Trust difficulties also subsequently hindered new friendships and romantic relationships (Short et al., 2017; Campbell et al., 2022), while victims withdrew socially and isolated themselves from family and friends (Aborisade, 2021; Henry et al., 2021). Cultural and religious norms further exacerbated isolation and stigma (Aborisade, 2021; Henry et al., 2021).

IBSA leads to job loss, forced job changes and fear of re-employment (Short et al., 2017; Bates, 2017). Victims incurred significant costs for legal representation and therapy. Some students dropped out or were expelled (Aborisade, 2021). Despite the severity of these harms, many victims did not seek help. Reasons for this included feelings of judgement, embarrassment, and victim-blaming (Campbell et al., 2020; Ruvalcaba & Eaton, 2020). However, some did report reaching out to police or helpline services (Short et al., 2017). Immigrants and refugees faced additional barriers: language difficulties, lack of digital skills, and inability to collect evidence (Henry et al., 2021).

Predictors of Victimisation

Studies are increasingly identifying the correlation between image-based sexual abuse (IBSA) and attitudinal or demographic characteristics across gender, age, sexuality, ethnicity, personality traits and prior victimisation (Karasavva & Forth, 2021; Ruvalcaba & Eaton, 2020; Eaton et al., 2022). The impact of gender on IBSA perpetration is mixed within empirical studies. Powell et al., (2020) identified 1 in 5 men (22.3%) reported having engaged in IBSA one or more times, as compared with 1 in 8 women (13.1%). Meanwhile, Karasavva & Forth (2021) did not identify gender as an independent predictor of NCII perpetration, although 75% of the victims identified their perpetrator(s) as male.

In a study by Eaton et al., (2022) of sextortion during the Covid-19 pandemic, men were more often targeted by threats to share intimate material. Younger adults (18–29 years) were also significantly more likely to receive threats of distribution compared with older groups (ibid). LGBQ+ individuals were more vulnerable to both non-consensual sharing and threats (Karasavva & Forth, 2021; Ruvalcaba & Eaton, 2020; Eaton et al., 2022). Native Alaskan, Indigenous North American, and African American women were disproportionately affected by threats to share images in the USA (Eaton et al., 2022). Similar findings were detected in a substantial cross-national survey of Australia, New Zealand and the United Kingdom (Powell et al., 2020). Reports were higher among Indigenous and ethnic minority groups: 35.9% of

12

Indigenous vs 12.2% non-Indigenous in Australia; 28.4% Māori vs 13.9% non-Māori in New Zealand; and 23.7% BAME vs 12.5% non-BAME in the UK (ibid).

In addition, harassment following IBSA was more commonly reported by men, ethnic/racial minorities, LGB+ women and individuals aged 16–19 compared to their respective counterparts (Powell et al., 2020). A survey of ten countries (Australia, Belgium, Denmark, France, Mexico, the Netherlands, Poland, South Korea, Spain, USA) also found that IBSA victimisation was significantly higher among LGBTQ+ individuals and those under 35, while overall rates were similar for men and women, with some country-level gender differences (Umbach, Henry & Beard, 2025).

Machiavellism, psychopathy, narcissism and sadism increased susceptibility to perpetration of IBSA (Clancy et al., 2019; Karasavva & Forth, 2021). Sexual and aggrieved entitlement were correlated with IBSA perpetration but were not independent predictors (ibid). A higher belief in victim-blaming increased IBSA perpetration risk, highlighting the need for education targeting IBSA myths (ibid). Moreover, prior experiences of sexual intimate partner violence predicted victimisation, whereas prior physical or psychological abuse did not (Eaton et al., 2022). Karasavva & Forth (2021) found that IBSA victimisation and perpetration are strongly linked: 28% of victims also perpetrated, and 57% of perpetrators had been victims. The authors caution that while this pattern resembles bully-victim dynamics, causality cannot yet be inferred. Significantly, none of these reviews mention prevalence of victimisation among sex workers.

Prevalence in the Sex Industry

While studies of the general population report high rates of IBSA victimisation—up to 1 in 10 adults in some surveys (Henry et al., 2019)—the sex industry faces disproportionate risk due to the inherently intimate nature of content creation and distribution. National Ugly Mugs (NUM), a UK charity driving sex workers' rights and safety, carried out a survey on image-based sexual abuse. The report found that:

- 91% expressed they were very or moderately concerned about IBSA.

- Over 55% of sex workers experienced IBSA violence through people they rely on for work (clients and prospective clients).

- 23.9% were outed as sex workers to friends/colleagues due to IBSA, 16.4% were outed to family, 16.4% were outed to neighbours and 7.5% were outed to school/place of education.

- 44.2% expressed that they contacted forums for removal of non-consensual content.

- 34.3% expressed that images were shared for content theft/fake profile use, 31.3% said images were shared to out them as sex workers and 23.9% said they were used to blackmail/shame/threaten them.

- Significantly, the largest group of individuals perpetrating IBSA against sex workers are clients, at 44.8%.

- 47.7% expressed that they were filmed or photographed without consent while working

(Redman & Waring, 2021)

This prevalence is magnified by the nature of platforms where sex workers engage with clients, such as subscription sites and content marketplaces. Digitally stored content has thus far been easily copied and traded, for malicious or salacious purposes. As a result, there is widespread concern among content creators within the industry. NUM's findings can be compared to a survey carried out for us by Thornhill Digital, for our whitepaper published in August 2025. Our participants also showed significant concern about IBSA, while further findings demonstrate an appetite for greater technological protections and a lack of trust towards platform safety.

- 100% worry that content will be leaked or shared without consent.

- 97% feel platforms should install technology to help trace leaks.

- 39% said they do not trust the platforms they work with to prioritise their safety as a content creator.

- 90% believe platform policies on safety are applied inconsistently or unfairly.

Taken together, these results highlight a deep unease among creators, reflecting the urgent need for stronger safeguards and more transparent prevention mechanisms. The scale of IBSA is global and growing, cutting across continents and borderlines worldwide, although the majority of the literature on IBSA is produced in the United States and Australia (Parton & Rogers, 2025). There are some findings which relate to sexual relationships or engagement online. Engagement in dating apps and coercive sexting increases risk of victimisation (Marcum et al., 2022). Normalisation of sexting and receiving unsolicited sexual images were associated with visitation of "slutpage" sites where IBSA is hosted (Clancy et al., 2021). Although academic articles tend not to name sex work explicitly, these patterns are particularly relevant for sex workers, whose economic survival often depends on digital self-presentation and content distribution. Downstream distribution—images being re-shared beyond the initial leak —and doxing can irreversibly expose workers to harassment, extortion and loss of income.

Accountability Mechanisms

_____

Efforts to prevent and respond to intimate image abuse (IBSA) remain fragmented and largely ineffective without robust accountability mechanisms. These mechanisms refer to the systems—technological, legal and institutional—that ensure platforms, perpetrators and policymakers are held responsible for preventing harm, responding to abuse and supporting victims. Platform shortsightedness and legal gaps continue to underestimate the impact for victims, particularly in the sex industry, where stigma and structural disadvantage amplify vulnerability. By examining current shortcomings and highlighting the need for enforceable standards such as online safety codes, we can begin to reshape accountability for image-based sexual abuse.

Platform Failures

_____

Many online platforms have failed to implement adequate controls to prevent, detect, or respond effectively to intimate image abuse. Notable shortcomings include: 1) Inadequate takedown processes as victims face protracted battles to remove content; 2) Weak identity verification, as perpetrators can create throwaway accounts; 3) Community guidelines are often poorly enforced, and even when platforms have policies in place, they frequently fail to proactively detect image-based abuse; 4) Profit incentives, as content hosts earn advertising revenue from viral, stolen sexual imagery; 5) Legal gaps across jurisdictions allow unregulated sharing of intimate content.

Research by Salter and Crofts (2015) highlights that adult-content platforms often lack consistent policies for addressing non-consensual content, leaving sex workers reliant on reporting mechanisms that are slow, retraumatising, or ineffective. In 2020, *The New York Times* reported that Pornhub hosted thousands of non-consensual videos, including images stolen from OnlyFans

(Kristof, 2020). The site failed to verify consent for years. Only after public outcry and advertiser boycotts did it implement more stringent upload controls.

Several concepts illustrate why platforms fail to protect victims. Downstream distribution makes it virtually impossible to remove images once they are shared, unless they are hashed (Kamal & Newman, 2016). Hashes (digital fingerprints of content) are often used by platforms to detect and automatically remove non-consensual content. But if content is flagged and hashed for takedown, it gets removed everywhere—including from the creator's own site—because platforms don't distinguish context.

In addition, "revenge porn" sites, "slut pages," and pornographic forums actively solicit stolen images for public commentary, sexual gratification and social status (Clancy et al., 2021; Maas et al., 2021). Motivations to share range from humour and social bonding to financial gain, coercive control and innate sexual desire (Davidson et al., 2019; Gauthier, 2023). Gulati (2025) argues that online misogyny and cybercrime persists due to weak platform accountability, driving the need to strengthen platform governance through stricter liability regimes, AI-driven content moderation, effective grievance redressal and regulatory oversight to safeguard women and deter abuse. In short, while some major platforms verify consent before hosting content, many lack automated detection tools to remove non-consensual images and provide inconsistent reporting processes, requiring victims to re-live trauma.

Our survey findings, published in our August 2025 whitepaper, show significant desire for greater platform accountability among online sex workers. This is demonstrable in the following results:

- 100% feel more loyal to platforms that demonstrate ethical leadership.
- 94% feel platforms are more focused on protecting their brand than protecting performers.
- 95% shared that a platform's stance on sex work affects whether they feel safe working with them.

- 93% feel exploited when platforms profit from their work but avoid speaking up about sex workers' rights

In addition, 100% agreed that a website certification system could help to create safer working conditions for online sex workers, while 100% shared that they would feel safer if sex workers were consulted during platform safety design. This offers two accountability mechanisms for platforms; the first is a certification system similar to the fairtrade movement that rates platforms based on their safety and workers' rights; the second is the assurance, as part of this certification system, that sex workers are consulted during the development of safety policies and design. Such an approach has already gained some momentum, given the Fairwork Foundation has recently co-developed a set of principles on which to rate sex work platforms (Warin et al., 2025). Fairwork evaluates companies' labour practices, with worker safety and data security part of the rating criteria (ibid).

Legal Gaps

Although legislation criminalising "revenge porn" has proliferated, gaps remain in consent definitions, as laws often require proving malicious intent or specific relationships. There's also issues relating to cross-jurisdiction enforcement (O'Hagan, 2023). Once images are online, they are rapidly distributed across borders. Victims may struggle to get injunctions or damages, while the lack of platform liability means that platforms claim safe harbour under intermediary liability laws. The redistribution of commercial intimate content on platforms outside the US Digital Millennium Copyright Act (DMCA), the UK's Online Safety Act 2023 (OSA), or other legal frameworks remains one of the most harmful and unregulated aspects of image-based abuse. These sites often operate offshore or anonymously, evade takedown requests and create a perception that non-consensual sharing is unstoppable.

The OSA in the UK is attempting to redress these grievances, by creating harsher penalties for platforms hosting IBSA and making the laws tougher on perpetrators. However, for sex workers,

these legal frameworks are further complicated by stigma and fear of criminalisation for their work. Reporting to police may expose them to discrimination, moral judgment, or prosecution for related offenses.

Legislation is further hindered by the complexity of motivation and behaviours. Many laws require proving a single, clear intent to harm, making prosecutions challenging (Parton & Rogers, 2025). Terms like "revenge porn" oversimplify the reality and reduce the impact (West, 2024). Typologies of offenders range from are characterised by both behaviour and criminal intent such as financial gain (Parton & Rogers, 2025), Intimately violent perpetrators motivated by control, transnational sextortion groups motivated by profit and individuals seeking amusement, social status, or sexual gratification (ibid). Moreover, legislation and policy differ across countries (ibid). Thus, current legal frameworks struggle to capture the breadth of behaviours (creation, distribution, threats), are slow to respond to technological developments like deepfakes and doxing and often place the burden on victims to prove intent and harm.

While sex workers are well aware that publicly posting content—such as on platforms like X (formerly Twitter)—effectively relinquishes any expectation of privacy or exclusive ownership, it is essential to distinguish between public and private digital spaces. In the UK, under Part 66C of the Sexual Offences Act 2003, content that has been publicly shared may fall outside the protections of image-based abuse laws, especially if the person redistributing the material *reasonably believes* it was publicly available and shared with consent. However, this exemption does not extend to content shared privately via encrypted messaging apps, subscription platforms, or direct messages, as it remains subject to an expectation of privacy under UK law.

The non-consensual redistribution of such private content, even by someone who claims a general belief that the subject has previously shared similar images publicly, may still constitute a criminal offence. Recognising this legal and contextual boundary is critical. Sex workers understand that public content is not protected under current UK law and do not expect tech companies like Image Angel to challenge this. Instead, the focus remains on combating the redistribution of private content, where the original context and consent were limited, and

ensuring that 'reasonable belief' is not misused as a blanket excuse for violating privacy and autonomy.

Given this confluence of high prevalence, platform inconsistencies in their policies and technological safeguards, as well as legal shortcomings, image-based sexual abuse remains a pervasive threat to sex workers' safety, autonomy and income. Protective technologies such as Image Angels' forensic watermarking provide critical interventions:

- Enabling evidence of origin and distribution paths.
- Supporting swift takedown requests by proving ownership.
- Acting as a deterrent by increasing the risk of identification for perpetrators.

This combination of technology, policy and survivor-led advocacy is essential to mitigate the harm of intimate image abuse in the adult entertainment industry.

Image Angel and the Deterrence of Abuse

_____

Image Angel is a digital deterrence tool that embeds invisible, non-removable forensic watermarks into visual content, enabling the traceability of unauthorised sharing and evidence capture to take action. This empowers victims with concrete, verifiable proof of misuse, shifting the burden back to perpetrators. As noted, IBSA that occurs on platforms beyond the reach of the DMCA, OSA, Digital Services Act, or other legal frameworks remains a damaging and largely unregulated domain of abuse. These platforms often operate anonymously or offshore, sidestepping takedown demands and reinforcing the belief that non-consensual sharing is untraceable and unpunishable.

Image Angel directly challenges this defeatist assumption. Even when content cannot be removed, Image Angel's forensic watermark survives the leak and remains tamper-resistant. It links the image or video back to a specific access event. When paired with contextual metadata, including who accessed the image and when, Image Angel enables source-level attribution even after a leak. This data is only made available if the platform or victim requests an investigation. In doing so, Image Angel restores agency to creators and platforms. This enables evidence capture for civil, criminal or platform-level action, especially where takedown routes fail.

Such an intervention is critical given a pervasive lack of trust in reporting channels. A survey of ten countries showed that many IBSA victim-survivors did not report or disclose their experience: only 38.8% reported to a platform, agency, or law enforcement, 14.3% disclosed informally, and 30.9% told no one. Across all actions taken, respondents were more likely to rate them as unhelpful than helpful (Umbach, Henry & Beard, 2025). Reasons for not reporting included shame, fear of being blamed or disbelieved, lack of evidence and a belief that nothing could be done — particularly when content had not been distributed. Others preferred to handle the situation privately or avoid further exposure.

As discussed, IBSA myths have been linked to perpetration. Karasavva et al. (2022) showed that acceptance of IBSA-related myths predicted a greater likelihood of tolerating or being willing to engage in such acts. IBSA myths are false or misleading beliefs that minimise the harm of IBSA, shift blame onto victims or justify the actions of perpetrators (ibid). Common examples include the ideas that victims are responsible if they shared intimate images, that such abuse is harmless or humorous, or that it is inevitable in the digital age—all of which serve to normalise, excuse, or even encourage non-consensual image sharing (ibid).

Technology can help to dispel such myths or, at least, reduce perpetrators' confidence in engaging in these behaviours. As noted, 97% of online sex workers shared that they feel platforms should install technology to help trace leaks in our recent poll. Image Angel is a technology-driven intervention designed to prevent, deter and trace the origin of image-based sexual abuse (IBSA). Core features include:

- Forensic watermarking of intimate content before content delivery network (CDN) distribution to identify the source platform even after scraping. This means we can tell which site it came from, even if someone uses tools to copy or alter it.

- Digital fingerprinting with a non-personally identifiable hex value[3] to trace leaks to the specific recipient on that platform. This means we can identify which account viewed and shared the content without knowing the person's real-world identity, though law enforcement can uncover that information if the survivor makes a complaint.

To address the predictors of perpetration identified in the evidence base—such as normalisation, enjoyment and myth acceptance—we call for a layered approach:

- Legislation, enforced by Ofcom in the UK, the eSafety Commissioner in Australia, the Federal Trade Commission in the US, or member states under the Digital Services Act,

---

[3] A **hex value** is a string of characters (numbers 0–9 and letters A–F) used to represent digital information in hexadecimal (base-16) format. In this context, it acts as an anonymous identifier, unique to each recipient's account, enabling traceability without revealing personal identity.

should ensure that *all platforms*, large and small, are legally obliged to adopt watermarking technology such as Image Angel to prevent and trace leaks.

- Government acknowledgment of a worker's rights certification system, like the Fairwork Foundation, with penalties for platforms that are rated poorly.

- Co-design of safety policies with sex workers on adult platforms.

- Governments and/or platforms to support online campaigns by helplines and survivor-centric NGOs targeted at teenagers.

- Mandatory video training on consent, safeguarding and the legal implications of sharing intimate images, when consumers sign up for or make accounts on adult-services platforms.

- Governments should promote offender-focused interventions, leveraging partnerships with civil society and NGOs. This includes highlighting the traceability of content, deterring intentional misuse and supporting therapeutic measures, including the intentional use of victim impact statements.

By combining prevention education with visible technical and legal safeguards, Image Angel aims to disrupt the cultural acceptance of IBSA while increasing perceived risk among potential perpetrators. Moreover, given that research shows sadism, narcissism, psychopathy and Machiavellianism are strongly associated with enjoyment and approval of sharing intimate images (Clancy et al., 2019; Karasavva & Forth, 2021), Image Angel can help reduce the sense of power offenders derive by demonstrating traceability and legal risk, while undermining social reward by increasing the likelihood of exposure.

Can Technology Prevent Abuse?

_____

While technology is not a panacea, it can *increase the certainty of consequences*, reducing the appeal of IBSA as an anonymous, low-risk offence. Public awareness campaigns and

widely-recognised technological deterrence such as Image Angel can undermine perpetrator behaviour by associating such conduct with reputational damage and legal exposure. This framework is consistent with situational crime prevention research, which holds that increasing the effort and risk of offending while reducing rewards can effectively deter harmful behaviour (Clarke, 1995). Increasing certainty of detection and social disapproval—combined with education—can deter opportunistic and status-driven perpetrators.

Several precedents illustrate how technology can prevent or reduce sexual violence. Microsoft's PhotoDNA is used by The National Center for Missing & Exploited Children (NCMEC) to hash-match[4] images of child sexual abuse material, while Videntifier can be employed for video content, reflecting the growing importance of detecting child sexual abuse material across both media types (Grossman et al., 2024; Lejsek et al., 2010). This has significantly reduced the circulation of illegal content by making it instantly identifiable. NCMEC's free *Take It Down* platform lets under-18s create secure digital fingerprints of explicit images or videos so platforms can detect and remove them without the files leaving their device (Henderson Vaughan, 2023).

Automated flagging systems on platforms like Facebook and Instagram detect non-consensual intimate images, with *specific reporting tools* and expedited takedowns (Henry & Witt, 2021). While this importantly shifts responsibility to platforms, prevents images from being viewed/shared and helps protect victims who may not know images are online, there are limitations (ibid). AI cannot always detect lack of consent without clear indicators. This is why interventions must tackle IBSA with multi-layered models of harm reduction, which systemically, holistically and technologically combat perpetration. Cultural change strategies such as education, platform policy and legal enforcement are also crucial.

Studies show that training which challenges myths about sexual violence reduces self-reported proclivity to offend (Yapp & Quayle, 2018). In sexual assault prevention, there are mixed

---

[4] **Hash-matching** is a digital technique that converts an image into a unique numerical "hash" or signature. Known illegal material can be identified by comparing these hashes across platforms, allowing detection of identical or altered files without storing or directly viewing the original content.

findings about whether higher perceived risk of detection correlates with lower perpetration intent, indicating *a need for more primary research about the impact of IBSA detection tools on perpetrator behaviour.* Bachman et al., (1992) found that sanction deterrence works for those who aren't already morally opposed to rape. Strang and Peterson (2013) identified that when men believed punishment was more likely, they reported a lower likelihood of using verbal coercion. However, this did not deter sexual assault via intoxication or force. Hahnel-Peeters et al., (2022) found the likelihood of being caught (high vs. low discovery) did not change men's self-reported rape likelihood.

However, it is possible, especially where digital violence is concerned, that perpetrators rely on perceived anonymity. Visibility and certainty of consequences disrupt this dynamic. Forensic watermarking heightens offenders' awareness that images are traceable to their source, reducing the confidence gained from perceived anonymity. In parallel, digital fingerprinting (hashing) enables platforms to detect duplicates and prevent further spread. Introducing watermarking technology and legal precedents in teenage education can challenge beliefs that IBSA is trivial or socially acceptable. Victims gain faster removal of content through automatic identification and takedown protocols, and mandatory consent training normalises the expectation that sharing intimate images is criminal and harmful. Determined perpetrators will attempt a series of methods to bypass or break a platform's safety technology, although doing so requires advanced technical proficiency. While technology and education cannot change sadistic or psychopathic traits in individuals, evidence capture can at least increase fear of consequences and empower victims to take action.

Large-scale deployment also requires partnerships with platforms and investment in infrastructure. In addition, without consistent international enforcement, some perpetrators may continue to share content via encrypted platforms. Effective implementation requires cross-sector collaboration between platforms, NGOs and law enforcement. This is why Image Angel has partnered with STISA (Survivors & Tech Solving Image-Based Sexual Abuse) in support of its global approach, which aims to connect NGOs and public authorities on the ground, alongside platforms and technology partners such as Image Angel.

Centering Survivors: Uniting All Stakeholders Against IBSA Through a Survivor-Focused Approach

---

Efforts to address perpetrator behaviour must go hand in hand with comprehensive initiatives to empower survivors. STISA's vision is to achieve a society where survivors of image based sexual abuse have a single point for reporting and requesting the removal of their abuse. Survivors are best supported by operational services such as local hotlines and helplines, operated by public authorities or NGOs, who speak their language, are well resourced, and understand the impact on their dignity in their culture or community.

To turn this vision in reality, STISA is focused on enabling these hotlines and helplines to have access to the professional solutions they need to analyse the content, process the reports from survivors and - with their consent - secure the removal of the abusive content and prevent its republication.

Hotlines and helplines are not run by technologists but by psychologists, lawyers and social workers. They rightly focus on supporting the victims, and therefore they treat technology as a secondary priority, which impacts negatively their response efficiency, technological scalability and the well-being of their staff[5]. If they are not equipped with the right set of technologies, they may earn the trust from the survivors, but they will not scale to the global nature of the digital world and the unlimited number of platforms disseminating abusive content.

STISA addresses this challenge by partnering with the trusted technology providers Videntifier and AbuseIO to offer two core solutions:

1. An abuse management solution, that enables the processing of reports from survivors and is available in 2 versions:

---

[5] On the importance of technology (case management and hashing technologies) to protect analysts, see the Point de Contact's White Paper *"Modération des contenus illicites en ligne – opérations et protection des professionnels : contenus terroristes et d'exploitation sexuelle de mineurs"* (pages 20–21, 2023).

- A hotline version that saves case managers time by automating the analysis of the reported information and issuing takedown requests to online service providers when appropriate. This frees up analysts to focus on tasks that are not automated, such as the legal determination of the content.
- A helpline version (under development), that enables case managers by automatically documenting the conversations with the people seeking assistance (typically through anonymous calls and chats), and issuing takedown requests when appropriate.

This solution is cloud-based, so the hotlines and helplines do not need to develop IT expertise and can focus on keeping full control of their relationship with the survivors.

2. A hash-sharing platform, that enables the effective removal of intimate content online by social media and service platforms at scale

While a handful of hotlines and helplines may have the capacity to interact with all the social media and hosting companies of the world, most of these organisations will not scale and will not be in capacity to support survivors efficiently. This is why using robust hashing algorithms and hash databases to store intimate content from survivors (with their consent), secure its removal and prevent its republication is a must.

STISA realised a Call to Action in the summer of 2025[6] that aims very pragmatically at raising the funds necessary to deploy at scale the technology solutions that hotlines and helplines need and that most of them do not have the IT expertise to develop.

The partnership with Image Angel follows the same logic: contributing to the global deployment of its watermarking deterrent technology by making it known and available to the survivors and the supportive organisations that are close to them.

---

[6] https://stisa.network/technology

Conclusion

This whitepaper argues that addressing intimate image abuse effectively requires an integrated approach—combining technological innovation with legal reform, stronger platform responsibility, and the leadership of those directly affected. Prioritising prevention and early intervention, rather than relying solely on punitive measures, holds the most promise for reducing incidence and safeguarding those at greatest risk. Image Angel's approach—combining technical deterrence, education and evidence capture—directly responds to key risk factors identified in the literature: 1) The appeal of IBSA as an enjoyable and status-enhancing act (Clancy et al., 2019); 2) Normalisation driven by IBSA myths (Karasavva et al., 2022).

While no single intervention can eliminate IBSA, the model we have proposed integrates proven prevention principles and holds promise as a multi-layered strategy to reduce harm and hold perpetrators accountable. In light of research demonstrating that IBSA is often motivated by misconceptions, power, control and social status, watermarking technology combined with evidence capturing, as operated by Image Angel, represents a foundational component for multi-layered deterrence Combining technical interventions (forensic watermarking), evidence capture, early education and mandatory consent training, this approach directly targets the predictors and motivations underpinning perpetration:

- It increases the perceived risk and consequences, particularly important in deterring opportunistic and socially motivated sharing.
- It challenges the myths and attitudes that normalise abuse.
- It supports victims with evidence-gathering tools and automated reporting pathways.

Actions to combat perpetrator behaviour must occur alongside wide-scale survivor empowerment. STISA is confronting the global scale of IBSA by equipping local services with accessible technologies and by supporting the development of a unified global infrastructure for intervention. Through its partnerships, hash-sharing protocols and cross-border technology

deployments, STISA supports a collective, international approach. Continued support for this global coordination is critical to making survivor-first responses both effective and sustainable.

In sum, Image Angel aligns with the evidence that reducing anonymity, disrupting cultural acceptance and increasing certainty of consequences are core to preventing crime. By embedding these principles into both digital infrastructure and social norms, the approach not only responds to current challenges, but also lays the groundwork for a more accountable and consent-respecting digital culture. Continued collaboration between technologists, policymakers, platforms and survivors will be critical to driving meaningful change and ensuring that protections evolve alongside emerging forms of harm. While a model of harm reduction may already be evident, it cannot achieve broad success without global collaborative efforts and legislative support from governments.

Bibliography

Aborisade, R. A. 2021. Image-Based Sexual Abuse in a Culturally Conservative Nigerian Society: Female Victims' Narratives of Psychosocial Costs. *Sexuality Research and Social Policy, 19*(1), 220–232

Bachman R, Paternoster R, Ward S. 1992. The Rationality of Sexual Offending: Testing a Deterrence/Rational Choice Conception of Sexual Assault. *Law & Society Review.* 26(2):343-372.

Clarke, R.V., 1995. Situational crime prevention. *Crime and justice*, *19*, pp.91-150.

Clancy, E. M., Klettke, B., & Hallford, D. J. 2019. The dark side of sexting-Factors predicting the dissemination of sexts. *Computers in Human Behavior, 92*, 266–272.

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).

Clancy E. M., Maas M. K., March E., Howard D., Klettke B. 2021. Just checking it out? Motivations for and behavioral associations with visiting "slutpages" in the United States and Australia. *Frontiers in Psychology*, 12, 671986.

Champion, A. R., Oswald, F., Khera, D., & Pedersen, C. L. 2022. Examining the gendered impacts of technology-facilitated sexual violence: A mixed method approach. *Archives of Sexual Behavior, 51*(3).

Davidson J., Livingstone S., Jenkins S., Gekoski A., Choak C., Ike T., Phillips K. 2019. *Adult online hate, harassment and abuse: A rapid evidence assessment*. UK Council for Child Internet Safety

Dardis, C. M., & Richards, E. 2022. Nonconsensual Distribution of Sexually Explicit Images Within a Context of Coercive Control: Frequency, Characteristics, and Associations with Other Forms of Victimization. *Violence against Women,* 1–22.

Eaton A. A., Noori S., Bonomi A., Stephens D. P., Gillum T. L. 2021. Nonconsensual porn as a form of intimate partner violence: Using the power and control wheel to understand nonconsensual porn perpetration in intimate relationships. *Trauma, Violence, & Abuse*, 22(5), 1140–1154.

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 US men and women. *Victims & Offenders,* 1–18.

Gauthier E. 2023. *Perceptions of Image-Based Sexual Harassment and Abuse: A Systematic Review* [Master's thesis, Queen's University]. qspace.library.queensu. https://qspace.library.queensu.ca/items/205aef0a-e650-4324-a9c2-462751814a71

Grossman, S., Pfefferkorn, R., Thiel, D., Shah, S., DiResta, R., Perrino, J. and Stamos, A., 2024. The Strengths and Weaknesses of the Online Child Safety Ecosystem. Available at: The Strengths and Weaknesses of the Online Child Safety Ecosystem: Perspectives from Platforms, NCMEC, and Law Enforcement on the CyberTipline and How to Improve It.

Gulati, R., 2025. CYBER CRIMES AGAINST WOMEN. Gender-Based Violence and Religion: Reinforcing Rights and Clarifying the International Framework, p.103.

Horntvedt, M.E.T., Nordsteien, A., Fermann, T. and Severinsson, E., 2018. Strategies for teaching evidence-based practice in nursing education: a thematic literature review. *BMC medical education*, *18*(1), p.172.

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

Henry, N., Vasil, S., Flynn, A., Kellard, K., & Mortreux, C. 2021. Technology-facilitated domestic violence against immigrant and refugee women: A qualitative study. *Journal of Interpersonal Violence,* 37(13–14).

Henry, N. and Witt, A., 2021. Governing image-based sexual abuse: Digital platform policies, tools, and practices. In *The Emerald international handbook of technology-facilitated violence and abuse* (pp. 749-768). Emerald Publishing Limited.

Hahnel-Peeters, R.K., Goetz, A.T. and Goetz, C.D., 2022. Do environmental cues to discovery influence the likelihood to rape?. Evolutionary Psychology, 20(4), p.14747049221141078.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.

Henderson Vaughan, E., 2023. NCMEC launches new service that can help you "Take It Down," *NCMEC.   {online   blog}   27   February.   Available   at:* https://www.missingkids.org/blog/2023/ncmec-launches-new-service-that-can-help-you-take-it-down (Accessed: 28 August 2025).

Kamal M., Newman W.J. 2016. Revenge pornography: Mental health implications and related legislation. *Journal of the American Academy of Psychiatry and the Law Online*, 44(3), 359–367.

Kulczak-Dawkins, R.P., Piroozfar, P.A. and Harder, M.K., 2018. A grounded thematic narrative literature   review   method.   *Building   Meaningful   Futures*. kulczak-dawkins-et-al-2018a-meth1-v2.3-gtn-lit-review-method.pdf

Kristof, N., 2020. *The children of Pornhub*. The New York Times, 4 December. Available at: https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html   [Accessed 30 Jun. 2025].

Karasavva, V., Swanek, J., Smodis, A., & Forth, A. 2022. From myth to reality: Sexual image abuse myth acceptance, the dark tetrad, and non-consensual intimate image dissemination proclivity. *Journal of Sexual Aggression,* 1–17.

Karasavva, V., & Forth, A. 2021. Personality, Attitudinal, and Demographic Predictors of Non-consensual Dissemination of Intimate Images. *Journal of Interpersonal Violence,* 1–25.

Lejsek, H., Þormóðsdóttir, H., Ásmundsson, F., Daðason, K., Jóhannsson, Á.Þ., Jónsson, B.Þ. and Amsaleg, L., 2010, October. Videntifier" Forensic: large-scale video identification in practice. In *Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence* (pp. 1-6).

McGlynn, C., Rackley, E., & Johnson, K. (2017). Image-based sexual abuse. *Feminist Legal Studies*, 25(1), 25–46.

Maas M. K., Cary K. M., Clancy E. M., Klettke B., McCauley H. L., Temple J. R. 2021. Slutpage use among US college students: the secret and social platforms of image-based sexual abuse. *Archives of Sexual Behavior*, 50, 2203–2214.

McGlynn, C., Johnson, K., & Henry, N. 2021. Beyond 'revenge porn': The continuum of image-based sexual abuse. *Feminist Media Studies*, 21(6), 887–902.

Marcum C. D., Zaitzow B. H., Higgins G. E. 2022. 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.

Moore, A. 2023. '"I stood up and fought back": how revenge porn survivor Georgia Harrison got her abuser jailed', *The Guardian*, {online} 23 October. Available at: https://www.theguardian.com/lifeandstyle/2023/oct/23/i-stood-up-and-fought-back-how-revenge-porn-survivor-georgia-harrison-got-her-abuser-jailed (Accessed: 31 July 2025).

O'Hagan, L. 2023. *The Human Element of Data Exploitation*. Queen's University Belfast. Online Thesis Available at: https://pure.qub.ac.uk/files/558880504/The_human_element_of_data_exploitation.pdf (Accessed: 31 July 2025).

Powell, A., Henry, N., Flynn, A., Scott, A., & J. 2019. Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample of Australian residents. *Computers in Human Behavior, 92*, 393–402.

Powell, A., Scott, A.J., Flynn, A. and Henry, N., 2020. Image-based sexual abuse: An international study of victims and perpetrators–A Summary Report. Available at: ImageBasedSexualAbuseReport_170220_WEB_2.pdf.

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

Paradiso, M.N., Rollè, L. and Trombetta, T., 2024. Image-based sexual abuse associated factors: A systematic review. *Journal of Family Violence*, 39(5), pp.931-954.

Parton, L.E. and Rogers, M.M., 2025. The predictors, motivations and characteristics of image-based sexual abuse: A scoping review. *Trauma, Violence, & Abuse*, pp.1-15.

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

Redman, S. and Waring, C., 2021. *Visual violence: Sex worker experiences of image-based abuses*. Manchester: National Ugly Mugs. Available at: https://nationaluglymugs.org/wp-content/uploads/2022/02/NUM-Visual-Violence-Report-FINAL_10022022.pdf [Accessed 17 June 2025].

Strang E, Peterson ZD. 2013. The relationships among perceived peer acceptance of sexual aggression, punishment certainty, and sexually aggressive behavior. *J Interpers Violence*. 28(18):3369-85.

Salter, M., & Crofts, T. (2015). Responding to revenge porn: Challenges to online legal enforcement. *Crime, Law and Social Change*, 62(3), 239–255.

Short, E., Brown, A., Pitchford, M., & Barnes, J. (2017). Revenge Porn: Findings from the Harassment and Revenge Porn (HARP) survey- Preliminary results. *Annual Review of CyberTherapy and Telemedicine, 15*, 161–166.

Umbach, R., Henry, N. and Beard, G., 2025, April. Prevalence and Impacts of Image-Based Sexual Abuse Victimization: A Multinational Study. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. (pp. 1-20.

West, J.R., 2024. Image-based sexual violence and imperfect victims: the case for platform cooperativism in the online sex industry. *Porn Studies*, pp.1-15.

Warin. R, Blake. P, Graham. M, Bertolini. A. 2025. Platform Sex Work: Working Conditions in the Online Sex Work Industry. Oxford, United Kingdom; Berlin, Germany.

Yapp, E. J., & Quayle, E. 2018. A systematic review of the association between rape myth acceptance and male-on-female sexual violence. *Aggression and Violent Behavior, 41*, 1–19.