

Virtual Violence and Harms Beyond the Screen: Gender-Based Cybercrimes, Escalating Offline Violence, and Institutional Neglect

Amber Hobbs*

Executive Summary

Gender-based cybercrimes have influenced and encouraged the continuum of sexual violence against women in both the virtual and the real world.¹ Image-Based Sexual Abuse (IBSA) is most commonly known as ‘revenge porn’, which acts as an umbrella term for the multitude of digital harms.² However, most people understand ‘revenge porn’ to mean the act of non-consensually sharing intimate images that were either taken without the victim’s consent, or the victim was unaware that they were being filmed at the time.³ Recently, IBSA has evolved exponentially with the use of Artificial Intelligence (AI) to create deepfake images, in which individuals have not consented or unknowingly had their faces digitally manipulated onto another’s body within an intimate image or video.⁴ Although the term ‘revenge porn’ is more commonly used, this paper adopts the term Non-Consensual Image Sharing (NCIS) instead. This is because the phrase ‘revenge porn’ implies that the victim has done something to incite revenge and thus is a term that is ostensibly victim-blaming.⁵ Not only have digital harms increased in different forms of image production and sharing, but some victims have unfortunately faced physical attacks offline by their online perpetrator.⁶ Additionally, heightened vulnerability of digital sexual violence is seen primarily within groups of young women and girls, showcasing intersectionality between age and

* Kent Law School, LLB with Honours Graduate, 2025. Email hobbs.amber@icloud.com

¹ Clare McGlynn and Erika Rackley, 'Image-Based Sexual Abuse' [2017] 37(3) *Oxford Journal of Legal Studies* 534-561

² Ibid.

³ Ibid.

⁴ Rangita de Silva de Alwis, 'A Rapidly Shifting Landscape: Why Digitized Violence is the Newest Category of Gender-Based Violence' (2024) 25 *La Revue des Juristes de Sciences Po* 62-72.

⁵ McGlynn and Rackley (n1).

⁶ Megan O'Brien, 'Online violence: real life impacts on women and girls in humanitarian settings', *Humanitarian Law and Policy* blog, 4 January 2024. Available at: <https://blogs.icrc.org/law-and-policy/2024/01/04/online-violence-real-life-impacts-women-girls-humanitarian-settings/> (last accessed 2 September 2025).

gender.⁷ All of this has been allowed to accelerate due to hopeless legal reform and ignorance by legislators to implement mechanisms that effectively combat evolving tools by perpetrators to inflict such harms.⁸ Such tools, including mass distribution on public platforms and AI, produce an accessible opportunity to commit such crimes, especially the availability to do so without substantial surveillance and proportionate legal punishments.⁹

1 | Timeline: Non-Consensual Image Sharing to Deepfakes

IBSA has been used by perpetrators since the 1980s. For example, Hustler Magazine included a section titled ‘Beaver Hunt’: this allowed anyone to share intimate images, provided a consent form was present.¹⁰ However, this was often used by past or current partners (typically men) to embarrass and shame the victim (typically women), especially since Hustler Magazine itself did not exercise meaningful duty of care and caution in verifying that consent was present.¹¹ For example, two cases brought against the company showcased the risk that the use of forged consent forms was substantial and often resulted in psychological and physical harms to the victim; especially when personal information was included with the photo.¹² Later, in the early 2000s, Mark Zuckerberg began his digital networking career when he created the website FaceMash to compare female students’ physical looks within elite American Colleges.¹³ While this did not involve IBSA, it reflected historical power imbalances between men and women, where technology was used to weaponise and amplify existing forms of objectification, thus triggering the normalisation of ill-behaviour against women.¹⁴

⁷ Olga Jurasz, ‘OU research reveals shocking level of online violence experienced by women and girls across the UK’, *News from The Open University* blog, 7 September 2023. Available at: <https://www.open.ac.uk/blogs/news/around-ou/university-news/ou-research-reveals-shocking-level-of-online-violence-experienced-by-women-and-girls-across-the-uk/> (last accessed 9 September 2025).

⁸ Women and Equalities Committee, *Tackling Non-consensual Intimate Image Abuse* (House of Commons, Fourt Report of Session 2024-25) 336.

⁹ Ibid.

¹⁰ *Gallon v Hustler Magazine, Inc*, 732 F. Supp. 322 (N.D.N.Y 1990).

¹¹ Ibid.

¹² Ibid and *Ursula Ashby v Hustler Magazine, Inc*, 802 F.2d 856 (6th Cir.1986).

¹³ De Silva de Alwis (n4).

¹⁴ Ibid.

Both examples showcase the effect of exacerbating gender inequality in contemporary society, as seen in the commonplace use of NCIS and deepfakes. NCIS has long been problematic, but deepfakes are worsening the extent of IBSA, as these images can be created with AI and completely damage the victim's social reputation without their personal contribution to the making of the image.¹⁵ Thus, this timeline, by including significant examples, illustrates the persistence of the issue and the frequent consequences experienced by victims. Legislation and policy continuously contribute to the lack of protections for women and girls, as illustrated in the Hustler and FaceMash examples, in both digital and offline realms.

2 | Development of UK Cybercrime Legislation and Combating Evolving Tools

Before the enactment of the Online Safety Act 2023, section 33 of the Criminal Justice and Courts Act 2015, was the primary legislation that aimed to combat cybercrimes, but did not directly assist in gender-based cybercrimes specifically. Under section 33, the victim had to prove that the perpetrator disclosed private sexual photographs or films, with the intent to cause distress. This requirement to prove the perpetrator's intent was problematic with victims dropping their cases due to this once too common hurdle.¹⁶

This requirement to prove the perpetrator's intent was criticised and highlighted by Georgia Harrison during her own journey for justice following NCIS.¹⁷ Georgia Harrison campaigned and raised awareness on behalf of those who also experienced difficulty with proving the legally required intent as this was preventing justice for all.¹⁸ Harrison argued for the removal of this requirement, because the act of sharing without consent and the harm caused to the victim should be the focus, rather than the perpetrator's subjective intention.¹⁹ In her case, the perpetrator, Stephan Bear, was able to argue that his intention was for financial gain, rather than causing distress to Georgia. He had uploaded the video to OnlyFans, a subscription based social media platform

¹⁵ Ibid.

¹⁶ Women and Equalities Committee (n8).

¹⁷ Ibid.

¹⁸ Ibid.

¹⁹ Ibid.

mainly known for sexually explicit content. This reflects the broader pattern seen in digital crimes, where gendered harm is intended to cause distress, instead of monetary gain as the main objective.²⁰ In Harrison's case, the main intention behind her perpetrator uploading the intimate video was an act of revenge for the ending of their relationship, with the financial gain an additional 'benefit' to uploading the image on a subscription based website.²¹ Fortunately, the Online Safety Act 2023 repealed section 33 of the Criminal Justice and Courts Act 2015 and created a new base offence for sharing intimate images without consent, by removing the need to prove motivation of the intention to cause distress, and instead criminalises the distribution of NCIS.²² Although the Online Safety Act 2023 has resolved the issue of proving the perpetrator's intent, the Act is not beyond criticism in other respects.

One of the main priorities of introducing the Online Safety Act 2023, was not only to combat barriers faced by victims of NCIS, but to assist those in cases including deepfake images.²³ For example, in 2024, the BBC File on 4 interviewed 'Jodie' (a pseudonym), who was notified by an anonymous email account in 2021 of her face being digitally manipulated onto another woman's body in a sexual manner.²⁴ It was later discovered that her best friend was behind this, Alex Woolf, a Cambridge-educated composer and BBC Young Composer of the Year 2012, who previously supported Jodie through the online harassment; making the abuse particularly traumatising.²⁵ Despite having been convicted of taking images of 15 women, including 'Jodie', and uploading them to pornographic websites,²⁶ Woolf only received a suspended 20-week prison sentence, and was instructed to provide compensation to the victims.²⁷ This reflects that the justice system has minimised the harms that victims of IBSA face, and the lack of

²⁰ See further, Suleman Lazarus et al., 'Exploring the Value of Feminist Theory in Understanding Digital Crimes: Gender and Cybercrime Types' [2022] 61(3) *The Howard Journal of Crime and Justice* 381-398. Lazarus et al. utilise the Tripartite Cybercrime Framework to develop their feminist analysis of cybercrime types.

²¹ Ibid.

²² See Sexual Offences Act, section 66B (as amended).

²³ Women and Equalities Committee (n8).

²⁴ Kate West, 'I was deepfaked by my best friend', *BBC News*, 2 April 2024. Available at: <https://www.bbc.co.uk/news/uk-68673390> (last accessed 2 September 2025).

²⁵ Ibid.

²⁶ Ibid.

²⁷ Antoinette Raffaella Huber, 'Image-based Sexual Abuse: Legislative and Policing Responses' [2023] 25(3) *Criminology & Criminal Justice* 736-752.

recognition for the seriousness of deepfake technology.²⁸ Harms include fundamental violation to one's individual right to dignity, privacy and sexual autonomy, even in the absence of physical coercion.²⁹ Thus, the creation and distribution of deepfakes by primary and secondary perpetrators further contributes to the continuum of sexual abuse due to ineffective legal frameworks.³⁰ These frameworks still diminish the impact of tangible harms arising from such violations, as those responsible for the creation of such frameworks choose not to recognise the severity of the abuse.³¹ For example, 49% of perpetrators feel safe when committing IBSA by virtue of online anonymity, including the ease of posting images without repercussions felt by 47%.³²

'Jodie' made further criticisms of the Online Safety Act 2023 due to it criminalising the sharing of deepfakes, but not their creation.³³ This is regrettable but is perhaps due to the fact that the 2022 Law Commission Report did not recommend the criminalisation of the making of deepfake images.³⁴ The Commission failed to acknowledge the significant risks involved, such as the potential for future distribution or images that are leaked due to hacking.³⁵ The assumption that no harm occurs when an individual's face is being unknowingly used fails to consider the chilling effect on digital security and personal autonomy. Thus, in enabling perpetrators to evade punishment, this dangerous loophole facilitates future exploitation and undermines protections against IBSA.

3 | Negligent Due Diligence in the Judicial Process and the Absence of Preventative Frameworks for Online-to-Offline Harms

The judicial process, from when the victim finds the courage to report to the police, to the possibility of their case being heard in court, remains deeply flawed.³⁶ Developments with legislation have proven useless in practice, as the police continue with poor professionalism when interviewing the victim, to the criminal court system

²⁸ Kim Barker and Olga Jurasz, 'Online Misogyny: A Challenge for Digital Feminism?' [2019] 72(2) *Journal of International Affairs* 95-114, 106-108.

²⁹ Ibid.

³⁰ McGlynn and Rackley (n1).

³¹ Barker and Jurasz (n28).

³² Jurasz (n7).

³³ Barker and Jurasz (n29).

³⁴ Non-Consensual Sexually Explicit Images and Videos (Offences) HL Bill (2024–25) 26.

³⁵ McGlynn and Rackley (n1).

³⁶ Women and Equalities Committee (n8).

itself leaving victims in fear of re-victimisation.³⁷ Firstly, specifically in regard to police officers who have been assigned to interview the victim, research suggests that justice is inaccessible as the conduct victims face deters them from bringing a case to court.³⁸ Some argue that insufficient funding in the UK's justice system hinders standardised training for interviewing vulnerable individuals, leading to misunderstandings.³⁹ However, while factual to an extent, the majority of police constables (62.5%) and inspectors (72.5%) are men in England and Wales (2024).⁴⁰ The number of men in such positions mirrors several experiences by victims, as interactions often include misogynistic perceptions, with some choosing to patronise the victim instead of supporting them.⁴¹ This exacerbates the already deep rooted gender inequality in society, both online and offline, including the mental and physical harms that victims continue to suffer due to the lack of competence in legal procedures.⁴² Secondly, victims are further disadvantaged by the court system's limited capacity to effectively respond to emerging forms of digital harm. For example, the Revenge Porn Helpline, introduced under the Criminal Justice and Courts Act 2015, noted the inadequacy of current judicial mechanisms in instances of IBSA.⁴³ Despite defendants being found guilty, perpetrators were given back their devices containing the images used against the victim, including when restraining orders were granted.⁴⁴ This level of absurd conduct essentially gives "back the weapon that caused the crime", meaning justice was diminished the second the device was returned.⁴⁵ Ultimately, once the whole process is finished, even if the perpetrator is found guilty, many victims feel that pursuing justice was pointless.⁴⁶ Not only does this prevent the sense of closure, but also leaves the

³⁷ North Yorkshire Police Fire & Crime Commissioner, '*Suffering in Silence*' (*Image-Based Sexual Abuse Report*) (North Yorkshire Police 2018). Available at <https://www.northyorkshire-pfcc.gov.uk/wp-content/uploads/2018/11/Suffering-in-Silence-Report.pdf> (last accessed 2 September 2025).

³⁸ D Clark, 'Distribution of police ranks in England and Wales 2024, by gender', *Statista*, release date 24 July 2024. Available at <https://www.statista.com/statistics/382525/share-of-police-officers-in-england-and-wales-gender-rank/#statisticContainer> (last accessed 2 September 2025).

³⁹ *Ibid.*

⁴⁰ *Ibid.*

⁴¹ *Ibid.*

⁴² Non-Consensual Sexually Explicit Images and Videos (Offences) HL Bill (n34).

⁴³ Women and Equalities Committee (n8).

⁴⁴ *Ibid.*

⁴⁵ *Ibid.*

⁴⁶ Barker and Jurasz (n29).

victim in a persistent state of anxiety about the risk of re-victimisation,⁴⁷ consequently reinforcing the psychological impact of the initial violation due to fear of the possibility that the images could be reshared.⁴⁸ Overall, these weaknesses not only discourage reporting, but also undermine trust in the legal system's ability to successfully address and prevent IBSA.

The majority of cybercrimes against women and girls usually stay within the online realm, with harms being felt by the victim psychologically.⁴⁹ However, there have been instances where such violence has moved offline.⁵⁰ Recently, the nation witnessed a horrific attack on a 15-year-old girl by Ellis Dismore, a 24-year-old man, who was found to have lied about his age to the victim on Snapchat.⁵¹ Beforehand, a relationship began online with the victim, but quickly ended due to NCIS and digital harassment.⁵² Later, after obtaining her home address, he attended her address and stabbed her, causing serious injuries.⁵³ This instance underscores the disturbing potential for digital violence to transition into physical harm in the real world.⁵⁴ In relation to Dismore's actions, there was insufficient intervention and preventative measures, such as Snapchat's failure to flag or intervene in abusive behaviour, to assist in deescalating the violence from transitioning into the real world.⁵⁵ There has been no statement by Snapchat responding to this specific situation, nor have they received any form of repercussion. The company's response within an Ofcom report in regard to protecting children online provides some insight towards the company's values and priorities.⁵⁶ Notably, the imbalance between upholding freedom of speech and the critical need to

⁴⁷ Ibid.

⁴⁸ Ibid.

⁴⁹ O'Brien (n6).

⁵⁰ Ibid.

⁵¹ Poppy Kennedy, 'Student found guilty of attempting to murder teen he met online in rage over being blocked', *Teesside Live*, 19 December 2023. Available at:

<https://www.gazettelive.co.uk/news/teesside-news/student-found-guilty-attempting-murder-28316320> (last accessed 2 September 2025).

⁵² Ibid.

⁵³ Ibid.

⁵⁴ North Yorkshire Police, Fire & Crime Commissioner (n37).

⁵⁵ Ibid.

⁵⁶ Office of Communications, 'Snap Inc Response: Ofcom Protecting Children from Harms Online', Ofcom, 26 July 2024. Available at:

<https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/284469-consultation-protecting-children-from-harms-online/responses/snap.pdf> (last accessed 2 September 2025).

safeguard children from harm raises significant concerns.⁵⁷ The company's response to Ofcom demonstrates concerns about over-censorship, but cases of grooming and sexual exploitation highlight the dangers of choosing to balance such actions, as prioritising unrestricted communication over child safety should not be up for discussion.⁵⁸ While the platform has implemented measures to reflect the aim of promoting connections, while limiting harmful content, the safeguards such as mutual friend requests can easily be bypassed through deception.⁵⁹ Thus, a present gap between intentional protections versus real-world risks, as seen above, illustrates a need to reassess such imbalances between free expression and safeguarding young users. Otherwise, failures in adequately preventing initial contact and harmful interactions demonstrate Snapchat's ignorance of the realities of online predation.

Online violence against young women and girls is shifting into offline violence, especially victims within a younger age bracket. For example, 7500 adults were surveyed, with one in ten women being victims of online abuse, and this increasing among 16-24-year-olds.⁶⁰ Although this age bracket cannot be applied to the victim of Ellis Dismore, it reflects the percentage among those under the age of 16. Recent findings showcase that a sixth of those who were victims of online harassment were under 18 years old, with girls under this age being the subjects of a quarter of reported offences of online blackmail in the UK.⁶¹ The Online Safety Act 2023 directly states that it wants to protect women and girls, especially those within younger age brackets, from online abuse and harassment.⁶² However, this stated intention has not provided material safeguards in practice following the introduction of the Act; this was the conclusion of the NSPCC in October 2024.⁶³ Data and statistics indicate that 19% of children aged 10-15 years had exchanged messages with someone they had never met before, including over 9000 child sexual abuse offences which involved an online

⁵⁷ O'Brien (n6).

⁵⁸ Ibid.

⁵⁹ Ibid.

⁶⁰ Non-Consensual Sexually Explicit Images and Videos (Offences) HL Bill (n34).

⁶¹ NSPCC Learning, 'Statistics briefing: online harm and abuse', NSPCC 2024. Available at: <https://learning.nspcc.org.uk/research-resources/statistics-briefings/online-harm-abuse> (last accessed 2 September 2025).

⁶² UK Government, 'Online Safety Act: explainer', GOV.UK, updated 17 March 2025. Available at: <https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer> (last accessed 2 September 2025).

⁶³ NSPCC Learning (n61).

element in 2022/23.⁶⁴ Additionally, those under 18 years old represented a sixth of those who experienced online harassment, including a quarter of those under this age bracket having reported offences of online blackmail.⁶⁵ This showcases that the Online Safety Act 2023 has not been effective, as proactive measures do not hold digital network companies and perpetrators accountable.

4 | Recommendations

4.1 Criminalise the Creation of Deepfake Images

Amendments should be made to the Online Safety Act 2023 to explicitly criminalise the creation of deepfake images without the individual's consent. Additionally, UK legislation should focus on implementing proportionate penalties that provide genuine justice for the psychological harms suffered by the victim due to the perpetrator's actions. A good example of this is Olympia's Law in Mexico, which criminalises both the creation and distribution of AI manipulated images; this legal advancement directly tackles deepfake-related abuse by targeting its production and dissemination.⁶⁶ In October 2023, a former student was charged with privacy offences after using AI to create non-consensual deepfake pornography, digitally undressing colleagues and profiting from the sale of these manipulated images.⁶⁷ Unlike the UK, Mexico has proactive legislation addressing such issues by explicitly safeguarding individuals from the creation and distribution of intimate images without consent, thus, anticipating AI-driven digital violence.⁶⁸

4.2 Police Interview Training and Psychological Screening

There should be mandatory specialised training for police officers to ensure standardised handling of IBSA cases. This training will not only improve officers' understanding of how to support victims effectively but also establish clear standards to hold officers accountable when their conduct falls below expected standards. For

⁶⁴ Ibid.

⁶⁵ Ibid.

⁶⁶ De Silva de Alwis (n4).

⁶⁷ Ibid.

⁶⁸ Ibid.

instance, this would include developing a victim-centred training programme on trauma-informed interviewing techniques to prevent secondary victimisation.⁶⁹ Training should help avoid victim-blaming and lack of empathy, which have been evident in deterring victims from reporting.⁷⁰ It would ensure that police officers understand the psychological impact of IBSA, including coercion and online harassment, while upholding transparency and accountability.⁷¹ Furthermore, the introduction of mandatory psychological screening for officers assigned to sensitive cases can ensure that necessary empathy, communication skills and trauma awareness are upheld.⁷² Assessments would be more effective if conducted by an independent body that oversees and assesses interview practices.⁷³ By analysing interview practices across different police forces and officers, the independent body could identify systemic issues or areas where further training or policy adjustments are needed. This would contribute to a continuous improvement cycle in police responses to IBSA.

Conclusion

Overall, the internet has become a weaponised tool, similar to a machinegun, where bullets, which represent the constant threat of social, psychological and physical harm, seem to be never-ending. This persistence highlights how such behaviour continues to thrive due to inadequate regulatory oversight and ineffective due diligence from legislators. If policymakers and public officials were willing to embrace meaningful reform, despite the initial rigid and logistical challenges, long-term solutions could be implemented to ensure significant justice and protection for all. Unfortunately, at this time, concrete recommendations for safeguarding young girls in digital spaces remain challenging.⁷⁴ Since privacy and data protection are frequently debated upon, there is more focus on individual rights over the need to shield vulnerable users from online harm.⁷⁵ This is likely because this area of crime is not collectively understood. Nevertheless, with the intense growth of awareness and advocacy to combat the barriers faced by victims within the legal realm, solutions are hopefully near. Continuous

⁶⁹ North Yorkshire Police, Fire & Crime Commissioner (n37).

⁷⁰ Ibid.

⁷¹ Clark (n38).

⁷² Ibid.

⁷³ Women and Equalities Committee (n8).

⁷⁴ NSPCC Learning (n61).

⁷⁵ Ibid.

pressure on legislators and the collective efforts of activists, educators, and policymakers, assist in reducing the disproportionate targeting of young women and girls by IBSA and additional harms faced due to the power of the internet, and ensuring instead that they are empowered and protected in digital spaces.