CHILDLIGHT

Global Child Safety Institute

# SEARCHLIGHT 2025

## Who benefits?

### Shining a Light on the Business of Child Sexual Exploitation and Abuse

HUMAN DIGNITY FOUNDATION

THE UNIVERSITY *of* EDINBURGH

UNSW SYDNEY

This document has been designed to be accessible.
If you require this document in an alternative format, such as large print or a coloured background, please contact us at childlight@ed.ac.uk or write to us at
Childlight Global Child Safety Institute, University of Edinburgh, Holyrood campus, Holyrood Road, EH8 8AQ

# SEARCHLIGHT 2025

## Who benefits?

### Shining a Light on the Business of Child Sexual Exploitation and Abuse

Established by

HUMAN
DIGNITY
FOUNDATION

Hosted by

THE UNIVERSITY
of EDINBURGH

UNSW
SYDNEY

# Foreword

The sexual exploitation and abuse of children is a global health crisis — one that governments and institutions around the world are increasingly recognising and addressing. But while progress is being made, it is not nearly fast enough. The world has mobilised before to prevent harm on this scale, as with Covid-19 and HIV/AIDS. We must do so again with urgency, because this pandemic is not inevitable — it is preventable.

Our latest Searchlight report into the nature of the crisis underscores the need for urgent action, shining a light on the financial networks that fuel child sexual exploitation and abuse (CSEA). The theme — who benefits? — asks a critical question: who is making money from this vile trade? The answer is as disturbing as it is clear. Organised crime groups profit, of course, but so do mainstream technology companies. Our research shows that advertising revenue increases when platforms attract high volumes of traffic, including traffic generated by offenders engaging in CSEA. The exploitation of children is not just an atrocity — it is an industry, generating billions of dollars in profits.

Other findings are equally sobering. Offenders are evolving, adapting and exploiting gaps in legislation and regulations. They groom single parents via dating apps to access their children. They target displaced children in conflict zones like Ukraine. And they trade images using sophisticated payment methods, including cryptocurrencies, to evade detection. We found that in these criminal enterprises, a child's worth is sometimes measured in mere pennies — the price of their suffering at the hands of an online predator. This is a market, structured and profitable, designed to generate revenue off the backs of vulnerable children. But markets can be disrupted, and that is where change must begin.

Searchlight, which complements our global index on the scale of CSEA, not only exposes these crimes: it provides solutions. It sets out how law enforcement and financial institutions can use telltale digital breadcrumbs to track and dismantle CSEA networks. Tech companies must be held accountable, pro-actively detect and remove child sexual abuse material (CSAM), and make more effective use of tried and tested tools, like blocklists, to shut down access to CSAM. Policymakers must act decisively, as the UK has begun to do, by criminalising AI-generated CSAM and banning so-called ‘how-to’ manuals for paedophiles. But much more must be done. We cannot afford to be complacent. This is not a problem to react to — it is one to prevent. Governments, businesses and communities must shift to a prevention-focused approach that stops CSEA before it begins, saving children from irreversible harm rather than scrambling to deal with the awful consequences.

Progress is possible. Prevention is possible. The world has eradicated diseases, tackled pandemics, and fought back against organised crime before. We must do the same here. The cost of inaction is the suffering of millions. And children can’t wait.

**Paul Stanfield**
Childlight CEO

# Contents

# Acronyms

| | |
|---|---|
| CI | confidence interval |
| CP3 | Canadian Centre for Child Protection |
| CRC | Child Rescue Coalition |
| CSAEM | child sexual abuse or exploitation material |
| CSAM | child sexual abuse material |
| CSE | child sexual exploitation |
| CSEA | child sexual exploitation and abuse |
| CSEC | commercial sexual exploitation of children |
| DNS | Domain Name Service |
| ECPAT | Every Child Protected against Trafficking |
| GBP | British pound sterling |
| ICMEC | International Centre for Missing and Exploited Children |
| INHOPE | Association of Internet Hotline Providers |
| ISP | internet service provider |
| IWF | Internet Watch Foundation |
| NCMEC | National Center for Missing and Exploited Children |
| NGO | non-governmental organisation |
| NSPCC | National Society for the Prevention of Cruelty to Children |
| OR | odds ratio |
| OSA | Online Safety Act |
| OSAEC | online sexual abuse and exploitation of children |
| P2P | peer-to-peer |
| PHP | Philippine peso |
| SCO | serious crime organisation |
| TF-CSEA | technology-facilitated child sexual exploitation and abuse |
| TOR | The Onion Router |
| UK | United Kingdom |
| UN | United Nations |
| USA | United States of America |
| USD | United States dollar |
| VPN | virtual private network |

# Introduction

Child sexual exploitation and abuse (CSEA) is prevalent in every country where it is measured and should be treated as a global public health emergency.

To better understand the nature of this crisis and help prevent it, Childlight has created the Searchlight series — a collection of innovative and timely studies published every two years, each exploring a different aspect of the problem. This series builds on Into the Light, our global index which measures the prevalence and magnitude of CSEA worldwide.

Since our launch in 2023, our research has uncovered troubling gaps in our understanding of how CSEA works, especially when it comes to the financial forces behind it. This report helps fill those gaps, shedding light on how perpetrators and organisations make money from the abuse of children. By exposing these hidden networks and dynamics, we hope to pave the way for stronger interventions and justice for victims.

In tackling the crucial question: Who benefits from CSEA? the 2025 edition of Searchlight presents eight new studies, focusing on three key areas — profitability, hidden at-risk populations, and accountability. The following summary describes each area and why it matters.

## Profitability: How do people make money from CSEA?

CSEA is not just a crime; it's a profitable business for many. In this part, we explore how individuals and organisations are making money from the exploitation of children. Three new studies dive deep into the financial side of CSEA:

> **Clicks for cash: The multi-billion-dollar exploitation of children. A rapid review of the economy of technology-facilitated child sexual exploitation and abuse (TF-CSEA)**
>
> **Where does the money flow? An exploratory study on the financial structures of organised crime linked to child sexual exploitation**
>
> **Following the money: Examining online financial behaviour to detect child sexual exploitation**

These studies expose the industries, financial systems and criminals who profit from CSEA. By understanding how the money flows, we can disrupt these financial networks and prevent further harm.

## Hidden at-risk populations

Some of the most at-risk groups and settings are less studied, yet they may experience CSEA. This part explores two under-researched areas:

> **Swipe wrong: How sex offenders target single parents on dating apps to exploit their children**
>
> **Hidden casualties of war:**
> **CSAM possession during humanitarian crises**

These studies reveal how emerging trends — like the misuse of dating apps to target parents or how humanitarian crises create hotspots for child sexual abuse material (CSAM) — are contributing to the global spread of CSEA. The key takeaway is that a one size fits all approach will not work. Prevention efforts must be tailored to these unique, evolving contexts. Our research offers concrete recommendations on how to address these complex, hidden drivers of abuse.

## Accountability: Who is holding perpetrators and systems to account?

We know that laws and regulations often fail to keep up with the ever-evolving nature of CSEA. Some perpetrators slip through the cracks, and even when they're caught, justice isn't always served. In this part, we explore how different systems around the world are holding — or failing to hold — people accountable. The three studies in this part are:

> **Legal challenges in tackling AI-generated CSAM across the UK, USA, Canada, Australia and New Zealand: Who is accountable according to the law?**
>
> **Unmasking exploitation: Study of Supreme Court cases reveals changing landscape of CSEA in the Philippines**
>
> **Access denied: How blocklists are thwarting attempts to view CSAM**

These studies highlight serious gaps, especially when it comes to new technologies like AI and the changing nature of abuse. However, there are also promising examples of success to build upon. For instance, blocking websites before perpetrators can access them is a strategy that's proven to reduce the spread of child sexual abuse material, showing that we can make a real difference.

## Why this matters

At Childlight, our mission is simple, but urgent: to protect every child from sexual exploitation and abuse. Understanding who benefits from CSEA financially, directly and indirectly, is essential to disrupt these perpetrators and the services profiting from children's suffering. By identifying the drivers of this illegal trade, we can begin to break the cycle of abuse.

The findings in this report show us where the biggest gaps are, what's working in the fight against CSEA, and where we need to take action. Now, it is time to move beyond the data. We must demand justice and the accountability of those who profit from the suffering of children, because children cannot wait.

# PART 1. PROFITABILITY

The exploitation and abuse of children is not only a crime, but a highly profitable industry, with offenders and organisations generating substantial revenue from abuse. This section explores the financial dimensions of child sexual exploitation and abuse (CSEA), examining how individuals and entities monetise harm through online platforms, financial transactions and organised criminal networks. Through insights from three new studies, we uncover the economic drivers behind CSEA, from financial sexual extortion to the commodification of child sexual abuse materials. Understanding these financial mechanisms is crucial to disrupting illicit profit flows, holding enablers accountable, and developing stronger safeguards to prevent further exploitation.

# Study A: Clicks for cash: The multi-billion-dollar exploitation of children. A rapid review of the economy of technology-facilitated child sexual exploitation and abuse (TF-CSEA)

## Introduction

Technology-facilitated child sexual exploitation and abuse (TF-CSEA) causes harm to its victims physically, emotionally and mentally, as well as financially. Applying a framework that looks at commercial determinants of health (Friel et al., 2023), we examine the financial and social economy of TF-CSEA. We review how societal norms have evolved to a point where profit extraction from the online abuse of children in all forms is overlooked due to the financial gain for companies and offenders (Schulz, 2018).

## Methodology

The following is a rapid review of both academic and grey literature pertaining to how offenders sexually abuse children through the medium of technology. This review looked at 20 publications across multiple disciplines, including big data reports, systematic reviews, discussion papers and qualitative studies. These reports largely focused on global subjects. However, some provided country-specific data from the United Kingdom, United States, India and the Philippines.

The review found that the profitability is largely split into three economies, based on the type of abuse and the technology it employs. These economies have grown so large that they are now estimated to represent a multi-billion-dollar industry. There are also signs of the behaviour being normalised outside of its financial gain, with children starting to exhibit similar behaviours in the push to create and collect sexual content of their peers.

# Research findings

The commodification of children involves the sale of child sexual abuse content (Acar, 2017; Malby et al., 2015), whether live or recorded, in addition to the threat of distribution of content by means of financial sexual extortion (C3P, 2022; ARU & IWF, 2024). In this way offenders have created concurrent economies, both of which victimise children and generate profit for the perpetrator from the abuse of the child. By utilising their networks on technology-facilitated spaces, offenders have created an economy for the sale and generation of child sexual abuse material (CSAM) that exists on both the Dark Web, the hidden part of the internet, and the clear web, which anyone can easily access using mainstream search engines. At the same time, they have found a way to monetise the private sexual images of children who have been sexually exploited by having children pay for their content not to be shared. These all have the same outcome: profit for the offender and for the systems that they use.

## Financial sexual extortion economy

One way in which offenders have created an economy for TF-CSEA is through financial sexual extortion, a victimisation scheme in which children and their families are the target of threats to share the sexual content of a child if they do not comply with monetary demands. One study found that, in some cases, there are recurring threats, even after the family has complied with the demands. To put this in context in terms of the magnitude and frequency of threats for payment that is being requested, the recently published Into the Light Index found that 3.5% of children globally had experienced sexual extortion in the last year, with 4.7% of children experiencing this at some time during their childhood (Fry et al., 2025). The global organisations that receive reports of TF-CSEA have also seen significant numbers of victims experiencing this crime. The Canadian Centre for Child Protection (C3P) received more than 2,600 reports of sexual extortion between September 2023 and April 2024 (C3P, 2024), the Internet Watch Foundation (IWF) received 176 in 2023 (IWF, 2023), and the National Centre for Missing and Exploited Children (NCMEC) received 26,718 reports also in 2023 (Vaughan, 2024). The numbers all point to the business of financial sexual extortion harming children across the world, regardless of their location.

Financial sexual extortion has created an economy out of the exploitation of children — and the financial gains not only accrue to the offender. By involving and misusing commercial enterprises, such as electronic service providers (social media, messaging apps and video call services) and online payment systems (money transfer services, cryptocurrency and online banking), these institutions become facilitators of the exploitation. Hence, these platforms play a role in the sexual exploitation and abuse that occurs on their services — services which have evolved to suit users — and by doing so they facilitate and enable the abuse to occur (Malby et al., 2015).

Of the more than 26,000 reports received by NCMEC concerning financial sexual extortion in 2023, the majority were directly reported by electronic service providers, which are mandated to report this type of crime on their platform; this may point to an awareness and acknowledgment of the part their platforms play. In one study (C3P, 2022), it was found that an overwhelming proportion of people experiencing financial sexual extortion were requested to pay their extorters through one particular online payment and money transfer service that does not require the sharing of bank details directly. Due to the fee structure of payments, this provided the company with a direct financial gain.

Social media platforms benefit financially as well, with increased content shared and generated on their platforms, increasing their use overall (Meggyesfalvi, 2024). According to Statista, spending by advertisers on social media platforms was approximately USD 116 billion in 2021, with projections from the World Advertising Research Centre that this will surpass USD 247 billion in 2024 (Statista, 2024; World Advertising Research Centre, 2024). As advertising is linked to the number of platform users, social media companies can make more money as more people use their platforms, including for purposes linked to the sexual exploitation and abuse of children. As a result, there is a financial gain for these sectors and for the offenders, which could be seen as a disincentive to regulate such activities, as this could impact negatively on advertising revenue. There are disincentives for protective regulation, as full operating costs are borne by the platform providers (Malby et al., 2015).

Beyond these streams, this crime has spawned the creation of fee-based companies that provide cybersecurity and reputation management services to victims to combat the offending extorters. These fees are often paid upfront and can amount to thousands of dollars. This only further commodifies the sexual abuse content of children by forcing them to pay for a solution to the crime of exploitation committed against them (C3P, 2022).

Technology with too few regulations has turned child sexual abuse into a highly lucrative industry.

## CSAM sharing economy

Offenders not only profit off the threat of sharing and the facilitation of TF-CSEA, but there is also a market for the sale of child sexual abuse, both recorded and streamed. Livestreaming and CSAM by request are two methods in which child sexual abuse material turns children into a commodity. One review noted that CSAM, especially new and offender-specified CSAM, is seen as collectable. There is also an appetite for known child sexual abuse material or abuse material on specific children.

Offenders will use technology-facilitated networking platforms to share memes or advertisements, which alert others to the availability of child sexual abuse content in exchange for payment or, in some cases, even about a child who can be targeted for sexual abuse (NCMEC, 2017; Ramiro et al., 2019). This advertisement of the sexual abuse material helps to further the representation of children as a commodity available for purchase (Roos, 2014). One video file of on-demand child sexual abuse can cost USD 1,200 (Malby et al., 2015), with the whole CSAM sharing criminal economy estimated to reach multiple billions of dollars annually (Acar, 2017).

Worryingly, this culture of collection is also appearing in the sexual behaviour of children with one another (ARU & IWF, 2024). In a joint project conducted in the United Kingdom, female youth described feeling pressured to send nude images, while male youth felt pressure to collect and distribute the sexual images to achieve higher social value (Reeves, 2023). Children reported using technology-facilitated sharing of intimate content as a means to explore and understand sexuality, which may provide a skewed version of sexuality that promotes the commodification of sexual expression (ARU & IWF, 2024).

## Livestreaming economy

The livestreaming of child sexual abuse, web-cam child exploitation and on-demand child sexual abuse material is an economy that provides remuneration to those it victimises as an incentive. In certain contexts, this becomes a means of financial independence or even livelihood. Children may be enticed to take photos of themselves to sell themselves or to connect in person with an offender to have their sexual abuse/exploitation recorded. Children have reported being paid USD 300 for 300 photos, in other circumstances they are provided with gift cards, material gifts or other items that they may not be able to purchase themselves (NCMEC, 2017). Girls are more likely to be offered these gifts and are subject to more sexualised discourse around their sexual exploitation (ARU & IWF, 2024).

In certain circumstances this is viewed as a line of work, which is passed down through generations (Ramiro et al., 2019). In some communities, children are simply being advised on how to self-produce sexual exploitation material to make money (Meggyesfalvi, 2024). Platforms like Omegle were misused as a place where children could be exploited and coerced into distributing their content for money (Meggyesfalvi, 2024). To demonstrate the magnitude of requests and pressure put on children, Terre Des Hommes developed a 3-D online model of a child, which garnered over 1,000 offers of financial compensation in exchange for performing sexual acts in 10 weeks (Acar, 2017).

# Conclusion and recommendations

The way in which companies are profiting from the sexual abuse and exploitation of children needs to be addressed. This will take changes to laws and regulations, as well as creating a financial penalty for non-compliance. This has started to occur in many locations in the European Union, United Kingdom and Australia. However, as the internet and connections via technology are global, this requires a more unified and global response to ensure that all children are protected. **Creating a standard fine system would help to address the current imbalance, in which there is no financial consequence for the role that companies play in facilitating and perpetuating the abuse.**

**In addition, the inclusion of TF-CSEA and its harm must be continued in internet safety discussions with young people, either through schools or awareness campaigns.** The use of technology to explore sexuality is the norm, but that does not mean that the acceptance of collecting sexual images of peers or feeling pressured to send them is also a part of that norm.

The relationship between the benefit to the offender and the cost to the victim shows that when offenders profit it is at the expense of the child. This problem goes beyond the individual platforms and involves internet service providers (Salter & Solokov, 2024) as well as app stores where the social media and messaging platforms are first made available (Prakash et al. 2021). **There needs to be greater regulation across all sectors involved, not just a focus on social media and messaging applications.**

It is only through identifying all of the entities that play a role in the exploitation and abuse of children that we can hope to stop it from occurring through the use of technology. **This requires specific legislative and regulatory powers to be provided to government and oversight bodies to mandate sectors such as app stores and internet service providers to use all the safety tools available.** These tools, which should be standard, such as photo matching, age assurance and moderation/response teams, are already a part of many social media and messaging services.

As more online safety-specific legislation is currently being enacted or drafted globally, it is an opportune moment to include such requirements. Sexual extortion, specifically, is a form of sexual exploitation that benefited from the Covid-19 pandemic, with technology facilitating the abuse across distance (Europol, 2020). In the end, however, it is the victims and their families who bear the cost of this system, no matter the perceived benefit, as both financial and non-financial costs are borne by the victims.

# Limitations

The nature of this report as a rapid review means that certain studies may have been missed during the course of the research. The study period (2014 to 2024) also meant that influential research prior to 2014 was not considered. The study did not consider all forms of child sexual exploitation and abuse and, as such, may have missed research that shows how money is exchanged in relation to the in-person sexual abuse of children.

## More information

**Suggested citation:** Stevenson, J., & Fry, D. (2025). Clicks for cash: The multi-billion-dollar exploitation of children. A rapid review of the economy of technology-facilitated child sexual exploitation and abuse. In: Searchlight 2025 – Who Benefits? Shining a Light on the Business of Child Sexual Exploitation and Abuse. Edinburgh: Childlight – Global Child Safety

**Researchers:** Mr James Stevenson, Professor Deborah Fry

**Registered study protocol:** OSF Registries | A Rapid Review of the Commercial Determinants of Technology-Facilitated Child Sexual Exploitation and Abuse (TF-CSEA)

**Ethics approval:** Not applicable

**Advisory committee members:** Dr Beverley Essue (Associate Professor of Global Health Systems, University of Toronto), Professor Nata Duvvury (Established Professor and Director Centre for Global Women's Studies, University of Galway)

**Funding acknowledgement:** The research leading to these results has received funding from the Human Dignity Foundation under the core grant provided to Childlight – Global Child Safety Institute under the grant agreement number [INT21-01].

# Study B: Where does the money flow? An exploratory study on the financial structures of organised crime linked to child sexual exploitation

## Introduction

This scoping review represents the first comprehensive examination of the economic and financial structures of serious crime organisations (SCOs) linked to child sexual exploitation (CSE). By synthesising academic and grey literature published between 2014 and 2024, alongside expert interviews conducted in Colombia, South America, this research provides crucial insights into the financial features, transactional characteristics, and supply-demand dynamics that fuel this illicit market. The study aims to inform criminal investigations and policy development by illuminating the operational economic patterns of SCOs engaged in CSE. The findings reveal the diverse structures of these organisations, ranging from small, localised groups to sophisticated transnational networks. The study also highlights the prevalence of business-like models employed by SCOs, their interconnectedness with other illicit markets, the preference for types of transactions that prioritise anonymity, the supply and demand influencing factors, and the critical need for a comprehensive, preventative approach to combatting CSE.

## Methodology

This analysis draws upon a detailed examination of 20 studies selected from an initial pool of 784 documents (528 academic articles and 256 grey literature documents), identified through a systematic search of relevant databases. The selection process involved a thorough screening of titles and abstracts, followed by an in-depth review of the full text of potentially relevant publications. To enrich the analysis and provide a deeper perspective on the phenomenon, 11 expert interviews were conducted in Colombia. Interviewees were selected based on their knowledge and experience investigating CSE in the country. The distribution is as follows: seven criminal investigators, one non-governmental organisation (NGO) expert specialising in CSE victim support, two former INTERPOL international police officers, and a prosecutor. The integration of these diverse perspectives provides a robust understanding of the complex operations of criminal organisations engaged in CSE.

# Research findings

## Corporate operational models in CSE

The structures of SCOs involved in CSE demonstrate considerable variability, ranging from small gangs to complex transnational networks (Kara, 2017; Taylor, 2019; Aronowitz & Veldhuizen, 2021). Additionally, SCOs frequently adopt business-like operational models, mirroring legitimate enterprises in terms of their focus on maximising profits and minimising costs (Krylova & Shelley, 2023; Aronowitz & Veldhuizen, 2021; Meyer, 2018; Demarest, 2015). These models often incorporate strategies related to recruitment, marketing, market segmentation, and financial management (Meyer, 2018; ECPAT, 2016; Hopkins et al., 2024; Palacios, 2022; Krylova & Shelley, 2023). The specific model used can be influenced by the cultural context and specific criminal group involved (Krylova & Shelley, 2023; Lugo, 2020; Palacios, 2022).

The literature also indicates that this business is characterised by low risk and exorbitant profits (Demarest, 2015; Lugo, 2020; Kara, 2017), despite the lack of reliable estimates regarding its overall market size. Estimates of the number of CSE victims vary widely, ranging from 945,000 to 12 million children (Miller-Perrin & Wurtele, 2017; Lasonder & Fiander, 2024). These discrepancies arise from differing definitions and methodologies, which hinder the production of accurate data on the phenomenon. In the digital realm, the Into the Light Index estimates that over 300 million children under 18 have experienced online sexual abuse and exploitation within the past year (Fry et al. 2024), underscoring the alarming scale and urgency of this issue.

Networks prioritise cash transactions and anonymous payment methods, making it difficult to trace their operations.

Analogous to that identified by Taylor (2018) in the United Kingdom, expert interviews in Colombia revealed a predominance of small, locally-operating organisations, typically comprising 3–5 individuals, with no apparent connections to larger transnational networks. The leaders of these organisations often have past involvement in sexual work and distribute responsibilities following a corporate structure, with defined roles such as recruitment, transportation, provision of locations, and control of victims. By delving deeper into this topic, experts indicated that the transnational trafficking of children for sexual exploitation is not highly prevalent due to strict border controls increasing the risk of apprehension.

## Links with drug and trafficking markets

Another finding is the potential link between CSE and other illicit markets, such as drug trafficking and human trafficking (Palacios, 2022; Kara, 2017; Krylova & Shelley, 2023). These connections may be due to the absolute dominance of a criminal group in a region, so that it appropriates all existing legal and illegal activities, or because groups seek to diversify their operations and markets. Nonetheless, expert interviews conducted in Colombia revealed a notable absence of direct links between SCOs involved in CSE and other illicit markets, potentially reflecting specialisation within criminal niches.

## Transaction methods and challenges to traceability

The transactions associated with CSE display substantial variation, depending on factors like the type of service, frequency, duration, victim's age and sexual experience, and the channel employed (ECPAT, 2016; Rai & Rai, 2021; Brown et al., 2022). For example, in Asia, perpetrators pay amounts ranging from USD 300 to USD 500 for sexual encounters with girls who have never had sexual intercourse before, but the price declines as the girls become more experienced (ECPAT, 2016). In Colombia, expert interviews indicated that the value of the abusive encounters could range from 200,000 pesos (USD 45) to 3,000,000 pesos (USD 669), depending on the profile of the victim and the perpetrator, with higher amounts paid by foreign individuals. Of the value of these encounters, the victim usually receives between 30% and 60%.

The predominant mode of transaction in these instances is cash, supplemented by the occasional use of mobile virtual wallets and bank transfers. This observation is consistent with the findings of Roche et al. (2023), who document the continued reliance on cash in physical encounters. This reliance potentially indicates a preference for anonymity and the reduced traceability afforded by cash transactions.

For the distribution and consumption of virtual abusive material, criminals use diverse payment methods to facilitate their operations and avoid detection, including currency remittance platforms, prepaid cards, and cryptocurrencies (Celiksoy et al., 2023; Hopkins et al., 2024; Roche et al., 2023; Krylova & Shelley, 2023). The channels through which perpetrators access the material include forums and specialised Dark Web sites, but also abusive livestream sites (Alianza Global WeProtect, 2021; Celiksoy et al., 2023; Van der Bruggen & Blokland, 2021). According to a report by WeProtect Global Alliance (2021), there are more than 3,000,000 accounts registered on the top 10 most harmful child sexual abuse sites on the Dark Web. Interviews in Colombia revealed that criminal groups often geo-block online content within the country where the exploitation occurs, restricting access in order to make it difficult for authorities to investigate.

> “It happens through specialised webcam sites. We face challenges with these platforms because, as you know, they operate using servers, which makes it easy for those managing these sites to display a child in another country, rendering them invisible in Colombia. Therefore, unless the information comes directly from a victim or a witness, detecting that this is happening becomes very difficult.
>
> (Personal communication,
> semi structured interview 19092024, 2024)

## Supply and demand dynamics

Demand for CSE is primarily concentrated among adult men and is driven by factors such as anonymity, perceived low cost, and the expectation of impunity in certain regions or countries (Demarest, 2015; Kara, 2017). According to Kara (2017), around 6% to 9% of males globally aged over eighteen engage in sexual exploitation with trafficked persons at some point each year. These factors contribute to the perpetuation of the market and emphasise the need for demand-reduction strategies. In Colombia, expert interviews highlighted a correlation between CSE and tourism, with higher prevalence reported in tourist areas such as Cartagena and Medellín.

The CSE victimisation risk is fuelled by the adverse conditions of children and adolescents, particularly those facing poverty, marginalisation, conflict, or displacement (Meyer, 2018; Rai & Rai, 2021; Wurtele, 2017; Lugo, 2020; Kara, 2017; Krylova & Shelley, 2023; Williams et al., 2021). These conditions create opportunities for exploitation and highlight the need for preventative measures. In Colombia, most of the victims are exploited through the desire for better living conditions and many without self-identifying as victims. This lack of self-identification, coupled with Colombia's age of consent being 14, significantly complicates prosecution.

> Tourists assume that [having sex with a 14-year-old child] is normal, that it is allowed because it was negotiated from abroad. They talk about it in a relaxed way [...] the issue of the age of consent. These people come  [mis-]informed that in Colombia, a person who is over 14 years old can have consented sexual relations [...].
>
> (Personal communication,
> semi structured interview 30102024, 2024)

## Conclusion and recommendations

This study represents the first comprehensive analysis of the economic and financial structures underpinning CSE globally. However, numerous further investigations, focusing on the specific dynamics in individual countries and regions, are crucial for developing effective interventions to combat it. The findings reveal that CSE is often perpetrated through sophisticated business models designed to maximise profits and minimise costs. This underscores the need for law enforcement and policymakers to adopt a business-oriented lens when confronting these crimes. The approach must target both the supply and demand sides of this illicit market, addressing the underlying factors that drive individuals to seek out CSE, while simultaneously tackling the conditions that leave children susceptible to exploitation.

Based on the findings of this study, the following recommendations are made:

**Recommendation 1.** Further research is needed to examine the economic and financial structures of SCOs involved in CSE in countries with the highest prevalence of CSE. Each case may present specific characteristics that were not addressed in this general review, but in all cases authorities should be encouraged to 'follow the money'.

**Recommendation 2.** It is essential to increase the age of sexual consent in Colombia. The current age of sexual consent is 14 years, which prevents the prosecution of this crime.

**Recommendation 3.** A thorough evaluation is recommended to determine whether investigations into cases of CSE are overly focused on local and isolated networks, potentially neglecting transnational networks that operate with greater sophistication. An economic analysis is advised to assess the perceived costs and benefits associated with different forms of CSE. This analysis could help identify modifiable determinants that reduce market demand or supply.

**Recommendation 4.** In some regions with a high prevalence of violence, collaboration among various crime investigation units is necessary to explore possible connections between CSE and other illicit markets, such as narcotrafficking. If such links are identified, it will be crucial to launch coordinated efforts to analyse the organisational context and structure of these networks.

**Recommendation 5.** A multidisciplinary and holistic approach to the prevention, investigation, and prosecution of CSE is necessary to address the complex economic structures it may present. This requires sharing lessons learnt and experiences from other countries and carrying out specialised interagency training that considers the underlying factors of the phenomenon.

# Limitations

This study has certain limitations that warrant consideration when interpreting the findings. Firstly, the sample is limited to a small set of countries where the economic and financial networks of serious crime organisations linked to CSE have been formally investigated. Furthermore, the identified studies employ diverse methodological approaches, samples, and objectives. Consequently, the results presented here should be considered suggestive, highlighting potential avenues for future research and deeper exploration, and are specifically attributable to the countries included in the sample. Secondly, the interviews were primarily conducted with criminal experts in Colombia, South America. While efforts were made to corroborate this information with other key stakeholders, the responses may be influenced by the predominantly law enforcement perspective of our experts. Although not strictly a limitation, this potential bias should be acknowledged when interpreting the results.

## More information

**Suggested citation:** Mojica, K., Harker, A., Norza, E., Gaitis, K.K., & Fry, D. (2025). Where does the money flow? An exploratory study on the financial structures of serious organised crime linked to child sexual exploitation. In: Searchlight 2025 – Who Benefits? Shining a Light on the Business of Child Sexual Exploitation and Abuse. Edinburgh: Childlight – Global Child Safety Institute

**Researchers:** Dr Arturo Harker, Mr Kevin Mojica, Dr Ervyn Norza, Dr Konstantinos Kosmas Gaitis, Professor Deborah Fry

**Study partners:** IMAGINA Center at Los Andes University, Colombian National Police – Office of Criminal Investigation, INTERPOL

**Registered study protocol:** OSF Registries | Where Does the Money Flow? An Exploratory Qualitative Study on the Economic and Financial Structures of Organized Crime Linked to Child Sexual Exploitation, with a Focus on Colombia and Latin America

**Ethics approval:** Universidad de los Andes (Acta No 001 de 2024 Alberto Lleras Camargo School of Government) and University of Edinburgh, Childlight Research Ethics Sub-Committee (WBCSE-AHR-24092024CL).

**Advisory committee members:** Milena Echeverry Campuzano (Coordinator of the Information System for Security and Coexistence [SISC] and leader of the Sexual Crimes Analysis Unit [UADS] at the Mayor’s Office of Medellín), Angélica María Garzón Alarcón (Dirección de Investigación Criminal e INTERPOL)

**Funding acknowledgement:** The research leading to these results has received funding from the Human Dignity Foundation under the core grant provided to Childlight – Global Child Safety Institute under the grant agreement number [INT21-01].

# Study C: Following the money: Examining online financial behaviour to detect child sexual exploitation

## Introduction

This is the first study to explore how online financial behaviour may indicate involvement with child sexual exploitation and abuse. A survey of almost 5,000 men in Australia, the United States of America (USA) and the United Kingdom (UK) found specific spending patterns among men who had sexual feelings towards children and those who had committed offences against children. Their online shopping, use of cryptocurrency, and other financial behaviour can help inform the efforts to detect child sex offenders. These findings are part of a larger context. According to The 2024 Crypto Crime Report by Chainalysis, child sexual abuse material (CSAM) "is an understudied part of the crypto crime ecosystem", highlighting evidence that "virtual currency is the dominant choice for buyers and sellers of commercial child sexual abuse content" (Chainalysis, 2024).

## Methodology

This study explored the connection between online behaviours and economic activities and men's sexual feelings towards and offences against children. Data was collected from 4,918 men in Australia, the UK, and the USA, with participants divided into three groups:

**No sexual feelings towards or offences committed against children (77.5% of participants)**

**Sexual feelings only towards children (11.5% of participants)**

**Committed sexual offences against children (11.0% of participants)**

The results are shown using odds ratios (ORs) and with a 95% confidence interval (CI). The OR shows how likely an event is to happen in one group compared to another group. The 95% CI is a range of numbers that shows where the true result is expected to fall 95% of the time if the study was repeated. If the range does not include 1.0, it means there is a significant difference between the groups. If the range does include 1.0, there is no clear evidence of a difference between the groups.

# Research findings

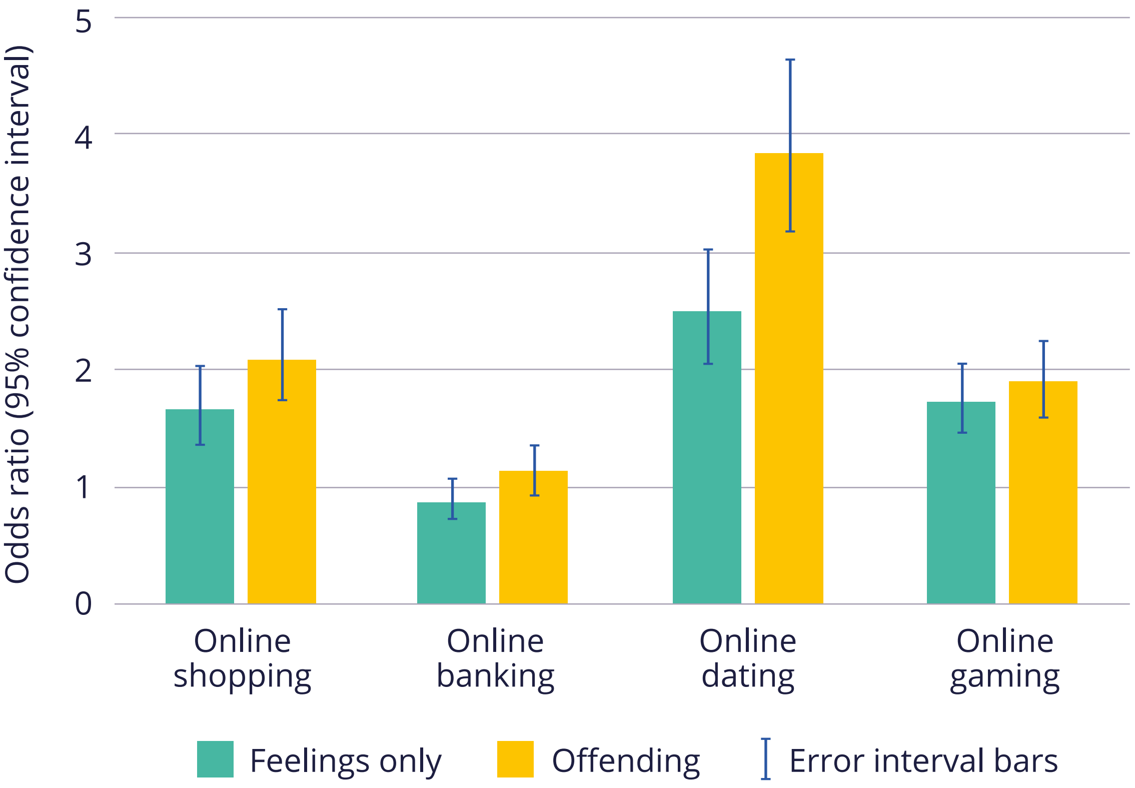
The study looked at four areas of online spending to understand potential financial patterns associated with sexual feelings or offences towards children: online economic activities, cryptocurrency ownership and use, purchasing sexual content online, and being approached online by someone selling sexual services.

## Online economic activities

Men in both the sexual feelings and offending groups had a higher likelihood of more frequent engagement in online activities, such as online shopping, online dating, and online gaming, compared to men with no sexual feelings or offences against children.

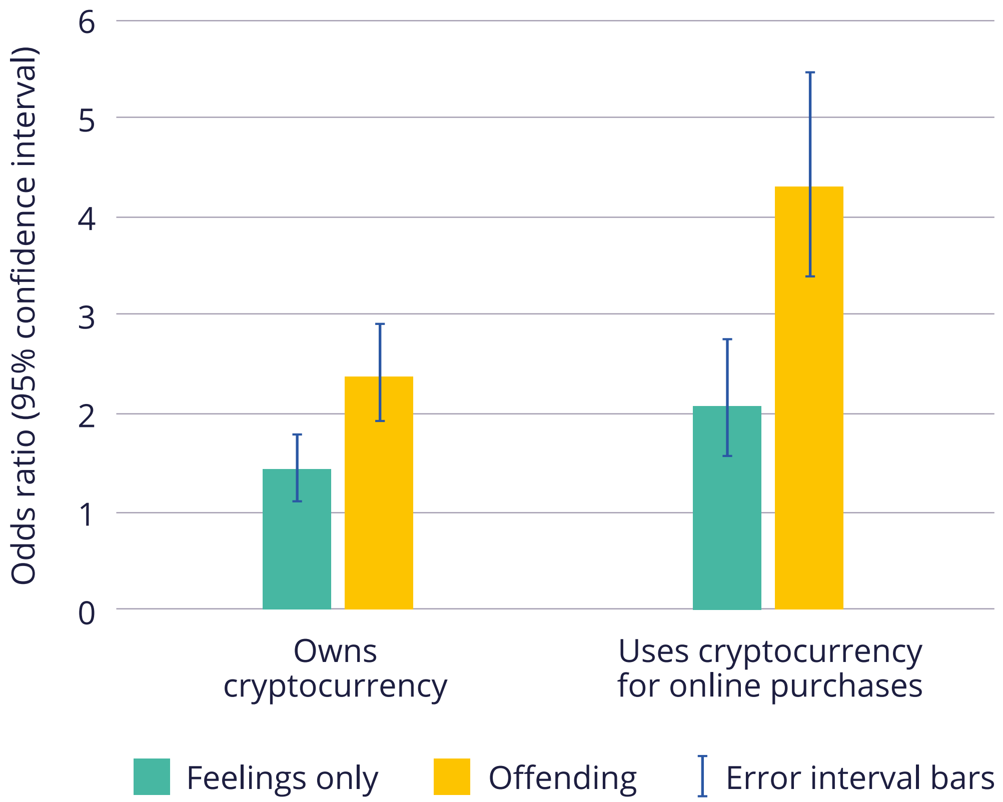
> **Online shopping: Those with sexual feelings towards children were 1.65 times more likely to shop online more often, while offenders were 2.09 times more likely to shop online more frequently, compared to other men.**
>
> **Online dating subscriptions: Men with sexual feelings towards children were 2.48 times more likely to use online dating sites more often, while offenders were 3.84 times more likely to use online dating sites more often, compared to other men.**
>
> **Online gaming: Men with sexual feelings towards children or who offended against children were 1.72 and 1.89 times more likely to play online games more frequently than other men.**

### Figure 1: Odds of online economic activity frequency



Digital footprints can help tackle hidden crimes.

## Figure 2: Odds of owning and using cryptocurrency



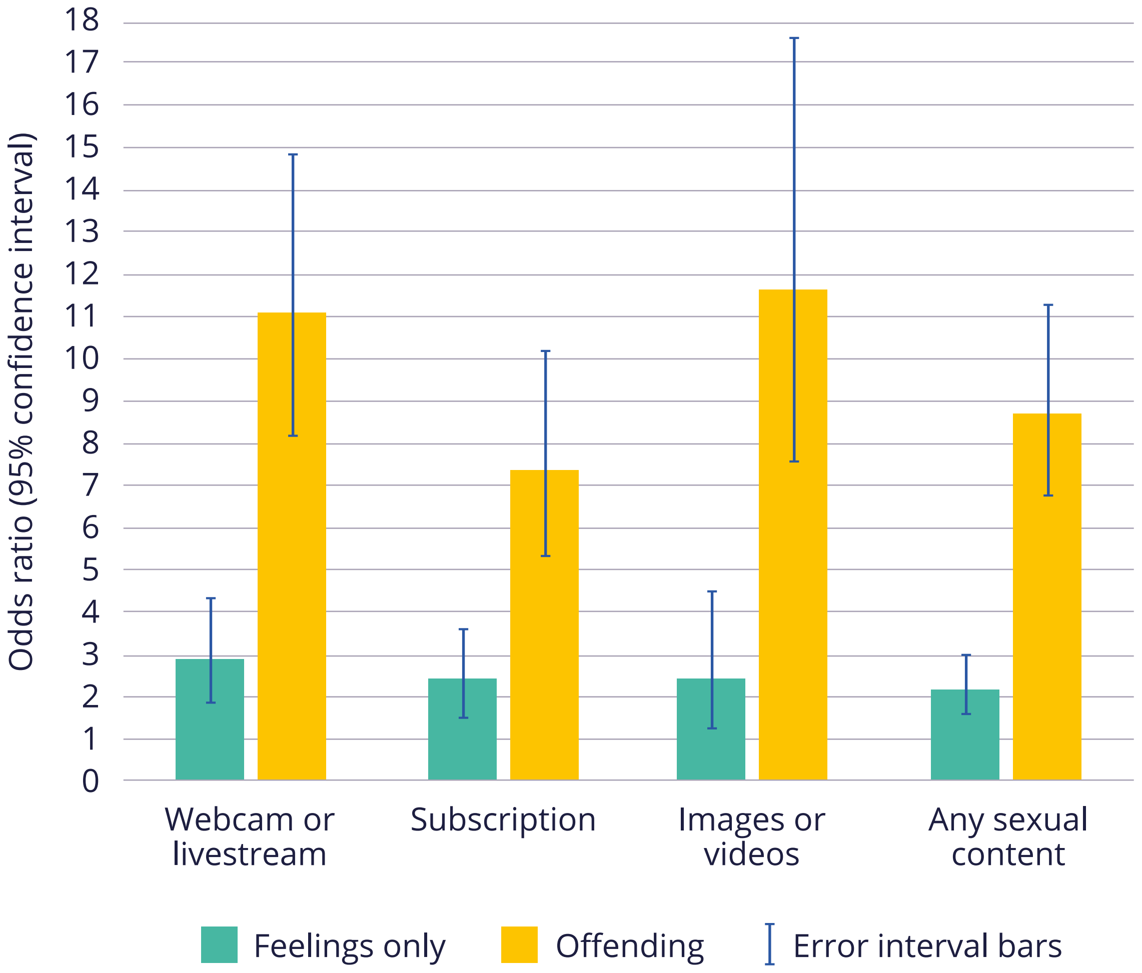
## Cryptocurrency ownership and use

Men with sexual feelings towards children were 1.42 times more likely to own cryptocurrency and 2.08 times more likely to use it for purchases, compared to other men. Offenders showed even higher rates, being 2.36 times more likely to own and 4.30 times more likely to use cryptocurrency for online purchases.

## Purchasing sexual content online

Men with sexual feelings towards children were about 2–3 times more likely to purchase sexual content, such as webcam services or nude videos, than other men. In contrast, offenders were 7–12 times more likely — with certain purchases, such as livestreams, 11 times more common. Offenders were much more likely than those with sexual feelings only to purchase all types of sexual content.

## Figure 3: Odds of purchasing sexual content online



## Approached online by someone exchanging their sexual abuse for money or other material gains

Men with sexual feelings towards children were 3.42 times more likely to be approached by a child exchanging their sexual abuse for money or other material gains, but showed no increase in the likelihood of approaches from adults. In contrast, offenders were 3 times more likely to be approached by adults and nearly 14 times more likely to be approached by children trading their sexual abuse.[1]

[1] Our survey asked about children "selling sexual services" to aid participant understanding. However, Childlight views the purchase of sexual services from a child as sexual exploitation in all circumstances.

# Conclusion and recommendations

Men who have sexual feelings toward children or who have committed sexual offences against children engage more frequently in certain online activities, like online shopping, dating, and gaming. They are also more likely to own and use cryptocurrency, with offenders having particularly high usage. Buying sexual content online is common among these groups, especially offenders. A significant risk factor for offending is being approached by someone offering sexual services (adults) or exchanging their sexual abuse for money or material gain (children). These online spending patterns could be a red flag to assist financial institutions and law enforcement in tracking child sex offenders.

These findings underscore that specific online financial behaviours, such as increased cryptocurrency use and frequent purchases of explicit content, can indicate potential for offending. For financial institutions and law enforcement, monitoring such patterns provides opportunities to identify and disrupt offending behaviours before harm occurs.

Recommendations for prevention include:

**Recommendation 1.** Expand financial monitoring. Many financial institutions are currently proactively seeking to detect payments associated with specific forms of offending against children such as livestreaming of sexual abuse or travelling for sex offending. However, the financial patterns associated with offending in this study suggest that detection processes could be sensitised to a broader array of suspicious transactions linked to offending risk.

**Recommendation 2.** Share information. The findings of the study point to cross-platform patterns of economic behaviour associated with child sexual exploitation and abuse offending across a range of services, including online shopping, dating, and gaming, cryptocurrency, and pornography. Enhanced information sharing between law enforcement, technology companies and financial institutions is critical to detecting these patterns and disrupting or intervening early in offending.

# Limitations

The study has several limitations. Participants were recruited through an online survey panel company, which may affect the generalisability of the findings. Additionally, because the study relies on self-reported data, there is a potential for social desirability bias due to the sensitive nature of the questions. Given the variation in the age of consent across jurisdictions and offence categories, the study defines a child as anyone under 18 when measuring online offending, which may have classified some legal sexual activities as illegal. Nonetheless, survey findings on the prevalence of sexual feelings and behaviours toward children are consistent with those of other studies.

## More information

**Suggested citation:** Salter, M., Whitten, T., & Woodlock, D. (2025). Following the money: Examining online financial behaviour to detect child sexual exploitation. In: Searchlight 2025 – Who Benefits? Shining a Light on the Business of Child Sexual Exploitation and Abuse. Edinburgh: Childlight – Global Child Safety Institute

**Researchers:** Professor Michael Salter, Dr Tyson Whitten, Dr Delanie Woodlock, Mr Matt Tyler, Ms Georgia Naldrett, Professor Jan Breckenridge, Professor Justine Nolan, Dr Noam Peleg

**Study partners:** Jesuit Social Services

**Registered study protocol:** OSF Registries | The nature of online offending against children: Population-based data from Australia, UK and the USA

**Ethics approval:** University of New South Wales (HC220317)

**Advisory committee members:** Ashley Katz (Director, Child Protection International Partnerships, National Office for Child Safety, Attorney-General's Department), Detective Superintendent Denzil Clark (Operations Coordinator, Queensland Police Service), Mark Dickson, Executive Manager, Financial Crime, Westpac Group), Dr Sarah Napier (Research Manager, OSEC Research Program, Australian Institute of Criminology), Carol Ronken (Director of Research, Bravehearts), Danielle Kelly (Head of Capacity and Prevention, ICMEC Australia)

**Funding acknowledgement:** The research leading to these results has received funding from Westpac as part of the Safer Families, Safer Communities Program. The work of the East Asia and Pacific Hub of Childlight at the University of New South Wales is supported by a collaboration agreement with the University of Edinburgh, under the core grant provided to Childlight – Global Child Safety Institute by the Human Dignity Foundation (grant agreement number [INT21-01]).

Click here for a related, more detailed report on Identifying and understanding child sexual offending behaviours and attitudes among Australian men.

# PART 2. HIDDEN AT-RISK COMMUNITIES

This section explores how financial motives drive the exploitation of children, revealing the hidden ways in which offenders and criminal networks profit from child sexual exploitation and abuse. It examines under-researched areas, including the misuse of dating apps to target single parents, the role of humanitarian crises in enabling online abuse, and the financial structures behind organised crime linked to this exploitation. Understanding these evolving threats is crucial to developing effective prevention strategies and disrupting the economic incentives that sustain these crimes.

# Study D: Swipe wrong: How sex offenders target single parents on dating apps to exploit their children

## Introduction

This study is the first to examine how frequently men with sexual feelings towards children, or those who sexually abuse children, use online dating platforms compared to other men. A survey of nearly 5,000 men across Australia, the United States, and the United Kingdom highlights the potential risk posed by child sex offenders who may target parents using these platforms to gain access to their children.

These findings contribute to a growing body of evidence about the misuse of dating platforms by offenders to exploit single parents. Recent research by the Australian Institute of Criminology underscores the heightened risk for single parents, particularly mothers, who use dating apps (Teunissen et al., 2024). Their survey of Australian dating app users found more than 12% of respondents received requests to facilitate child sexual exploitation and abuse, most often related to the respondent's own child. Similarly, news reports, including of a Scottish lorry driver who manipulated women via dating apps to gain access to their children in order to sexually abuse them, illustrate the tangible dangers these platforms can pose (Currie, 2024).

This emerging issue signals an urgent need for platform accountability and the implementation of safeguarding measures to protect single parents and, by extension, their children.

## Methodology

This study examined how frequently men use online dating platforms and whether their usage patterns relate to sexual feelings toward children or prior offending against children. The research is based on a survey of 4,918 men from Australia, the United Kingdom, and the United States. Participants were categorised into three groups:

**No sexual feelings towards or offences committed against children (77.5%)**

**Sexual feelings only toward children (11.5%)**

**Committed sexual offences against children (11.0%)**

Participants answered questions about their online dating habits, use of privacy tools, financial transactions, and engagement in other online activities. The study aimed to identify behavioural patterns that differentiate these groups and assess the risk factors associated with dating app use among offenders.

Associations were reported as cumulative odds ratios (ORs) with 95% confidence intervals (CI). The cumulative OR measures the likelihood of being at or above a certain category versus below it in an ordered outcome (i.e., online dating frequency), across different groups. The 95% CI represents the range within which the true OR is expected to fall 95% of the time if the study were repeated. An association is considered statistically significant if the CI does not include 1.0; if 1.0 falls within the interval, there is no statistical evidence of a significant difference between groups.

# Research findings

## Use of online dating platforms

Men who used online dating sites more often were 2.48 times more likely to report having sexual feelings towards children, and 3.84 times more likely to have sexually offended against children, compared to men who have no sexual feelings or have not offended against children.

**Two-thirds (65.8%) of men who had sexually offended against children, and more than half (53.9%) of those with sexual interests only, had ever used an online dating platform.**

**By comparison, online dating apps had only ever been used by less than one-third (30.6%) of men who have no sexual feelings or have not offended against children.**

**22.1% of men who had committed sexual offences against children used dating apps daily, compared to 14.5% of men with sexual feelings only and 8.1% of other men.**

More than one in five male abusers use matchmaking sites daily.

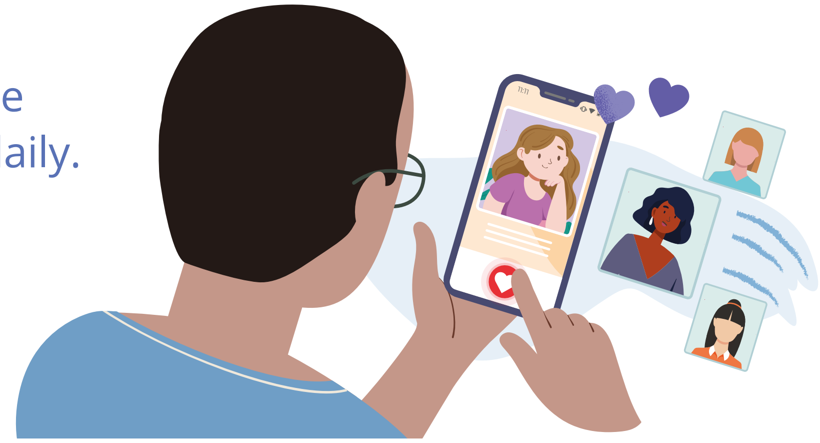
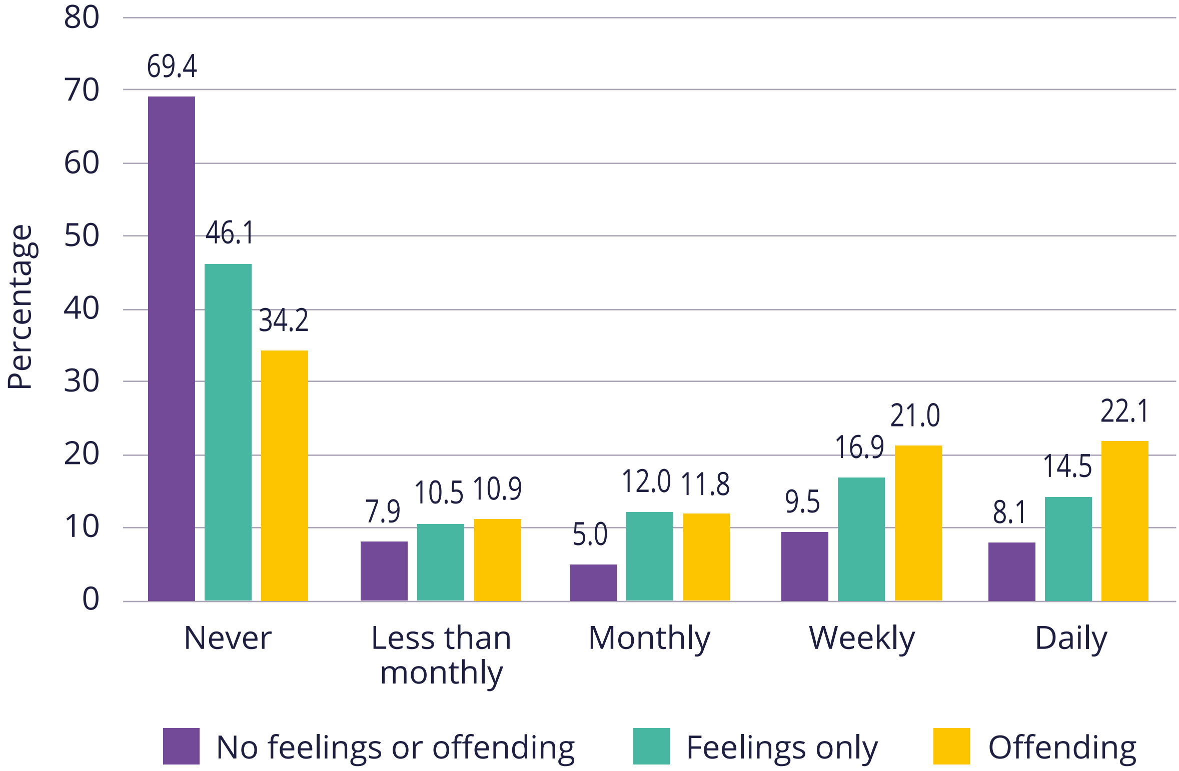


**Figure 1: Proportion (%) of men by online dating frequency**



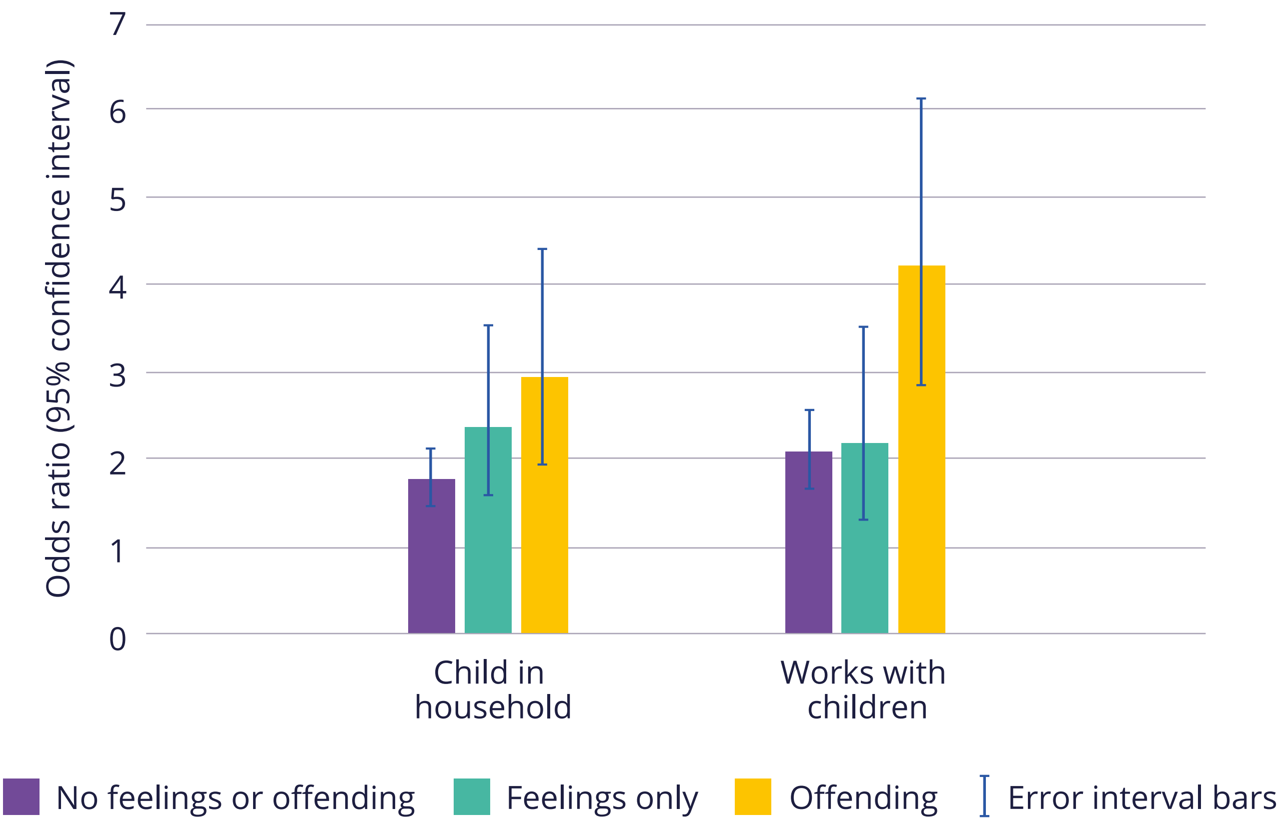
More frequent use of dating apps among men who had committed sexual offences against children was associated with a cumulative increase in the likelihood that they also had access to children.

**Offenders were 2.95 times more likely to live with a child.**

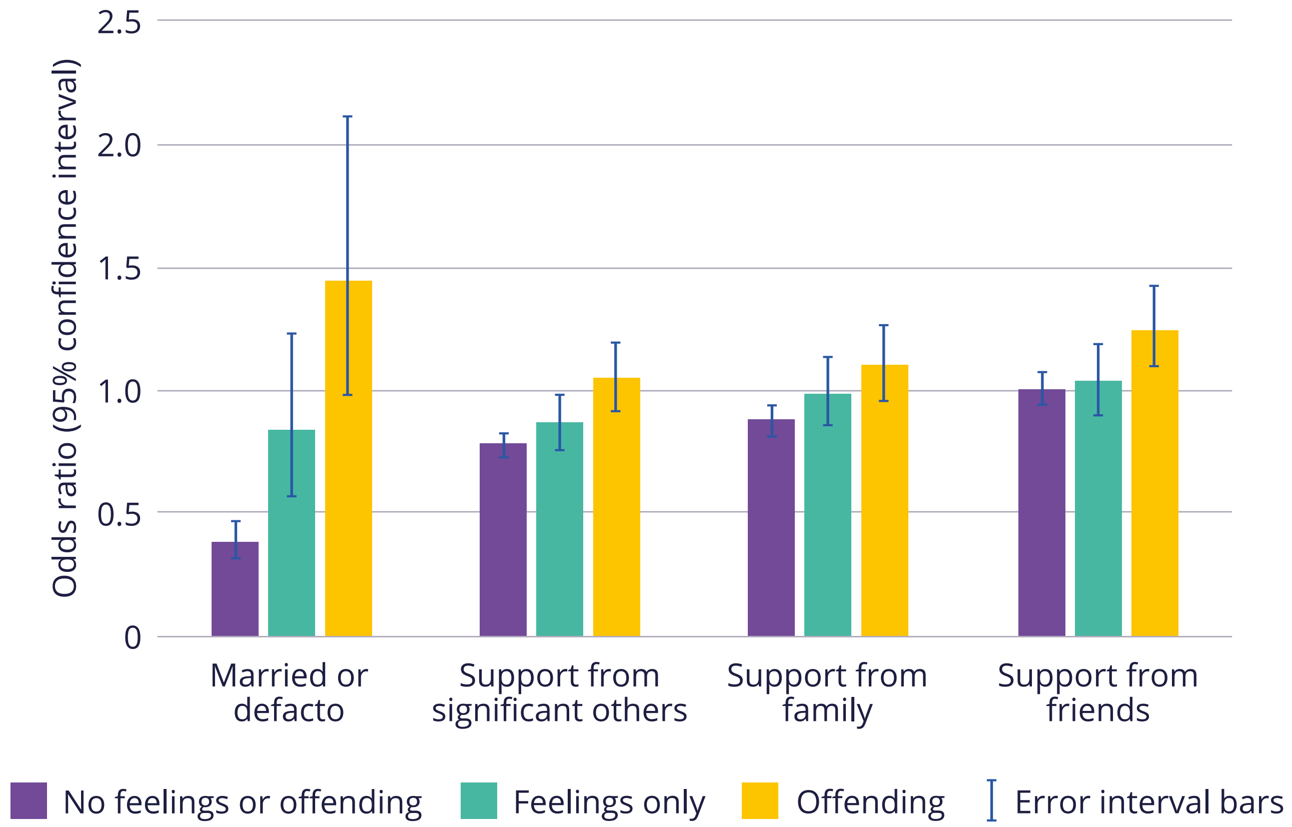
**Offenders were 4.18 times more likely to work in child-related professions.**

**Unlike non-offenders, who used dating apps less frequently if they were married or had strong social support, offenders showed the opposite trend — greater use of dating apps if they were married or had social support networks.**

## Figure 2: Odds of online dating frequency by demographic factors



### Figure 3: Odds of online dating frequency by social support

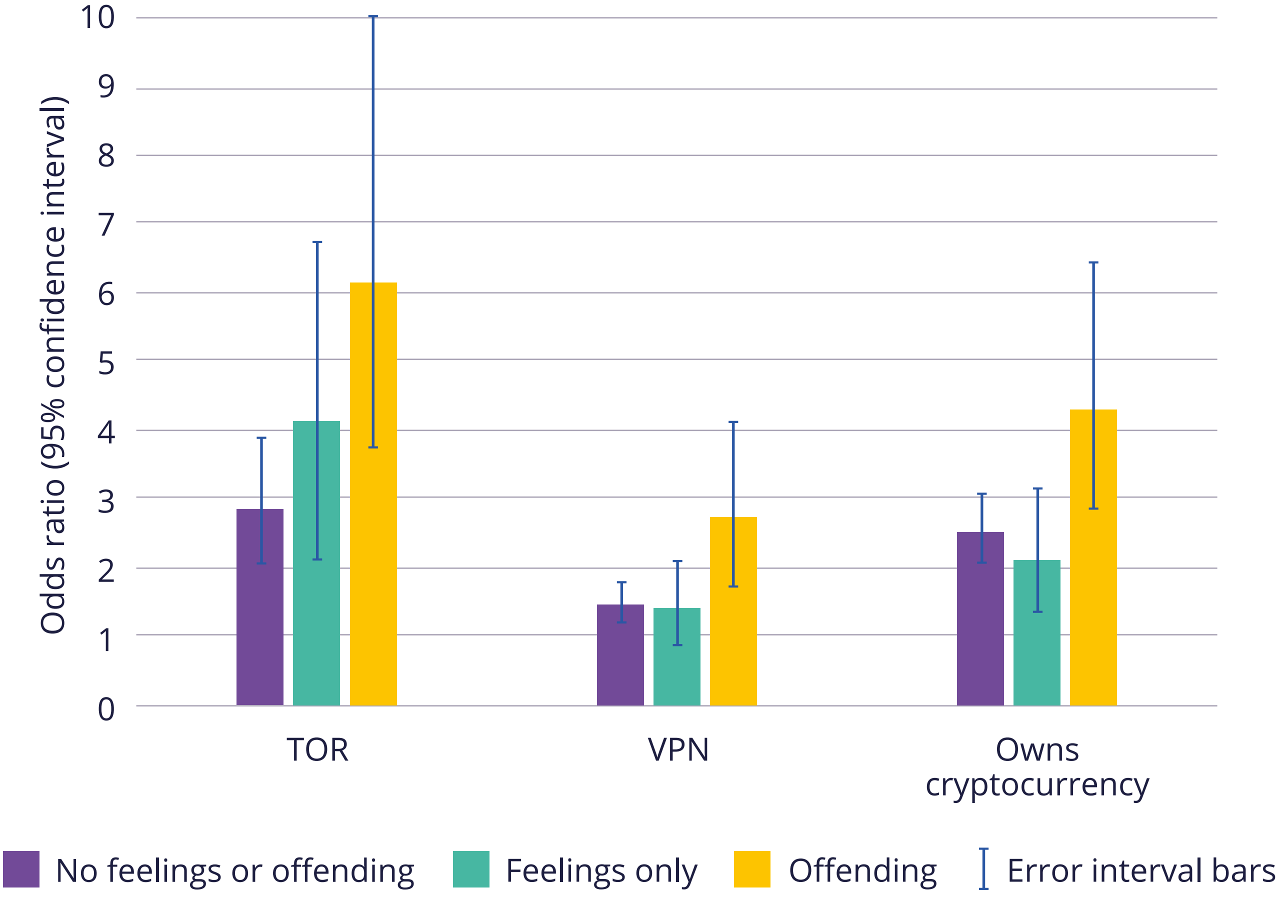


## Use of online privacy tools and financial transactions

Privacy and anonymity tools were commonly used by men who had committed sexual offences against children.

> **Offenders who used The Onion Router (TOR) (the Dark Web router used to access encrypted hidden webpages) were 6.14 times more likely to use dating apps frequently.**
>
> **Offenders who owned cryptocurrency were 4.31 times more likely to use dating apps frequently.**

### Figure 4: Odds of online dating frequency by use of privacy tools



## Use of pornography and online sexual services

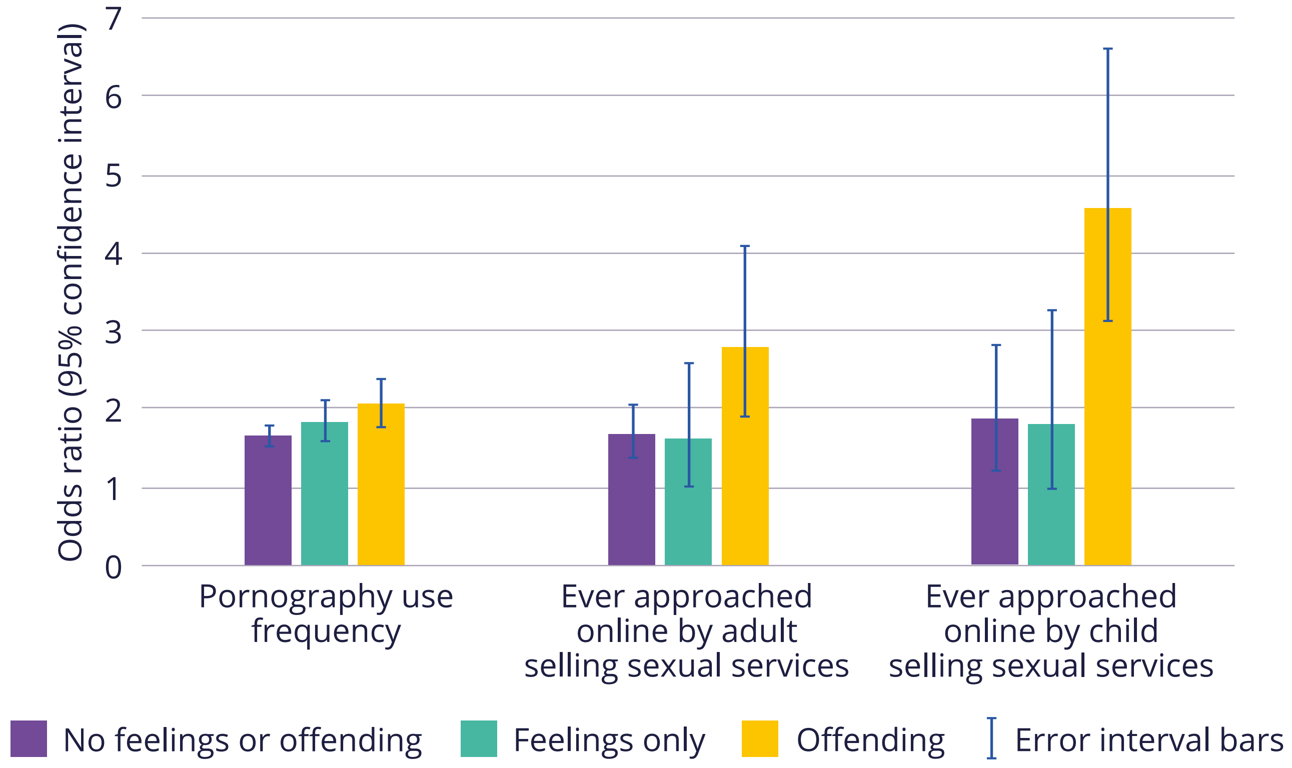
Consumption of pornography and engagement with online sexual services were linked to higher dating app use.

**Frequent use of pornography was linked to increased dating app use across all groups, with offenders having the strongest link (2.04 times greater odds).**

**Men who were approached online by adults selling sexual services (adults) or children exchanging sexual abuse for money or other material gains were significantly more likely to use dating apps frequently.**

**Offenders who were approached by a child exchanging their sexual abuse for money or other material gains were 4.54 times more likely to use dating apps frequently.**

## Figure 5: Odds of online dating frequency by pornography use frequency and ever being approached by person selling sexual services online[2]

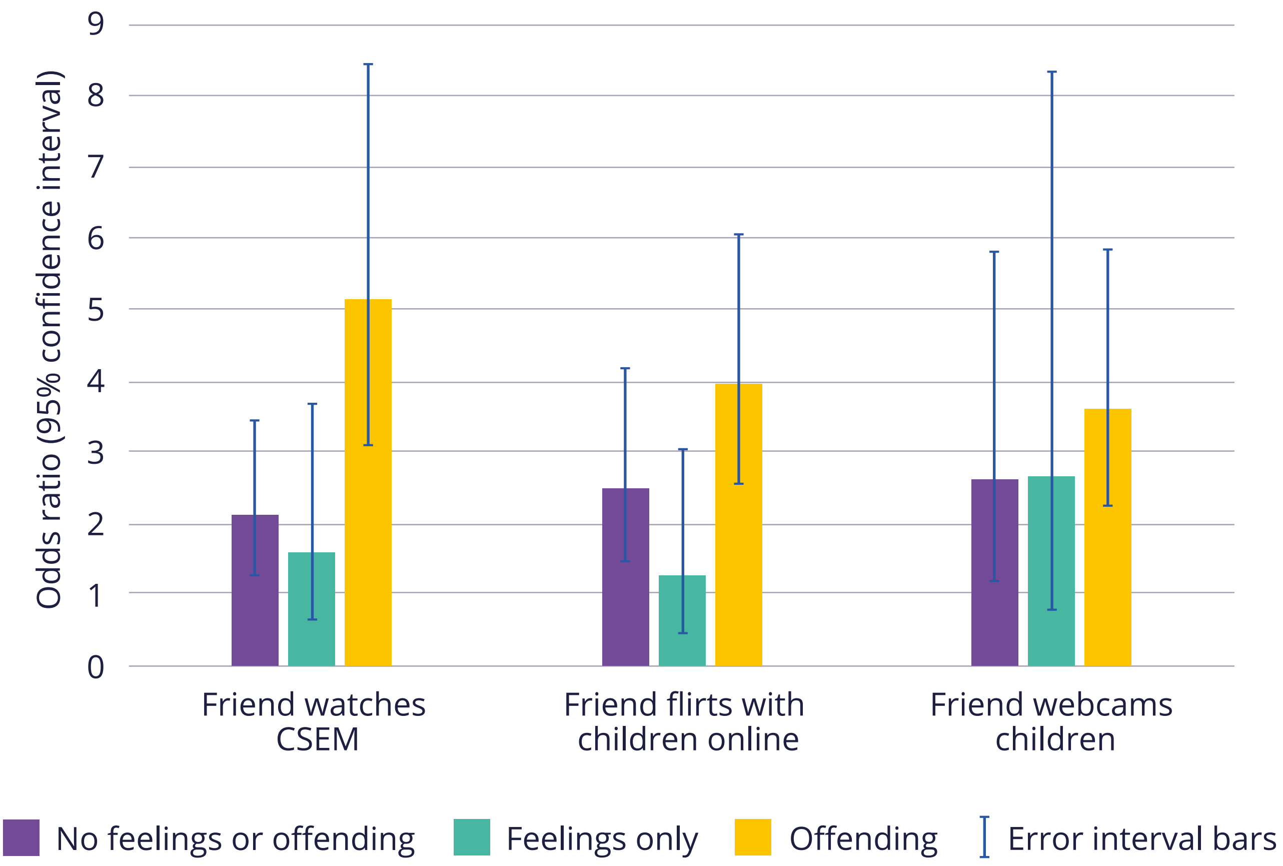


Online dating frequency was greater among men who had a friend who engaged in child sexual exploitation material (CSEM).

> **Among men who did not have sexual feelings towards children or who had not committed sexual offences against children, each increase in online dating frequency was associated with twice the odds of having a friend who views CSEM.**
>
> **Among men who had sexually offended against children, having a friend involved in CSEM was associated with a three to five times higher odds of greater online dating frequency.**

[2] Our survey asked about children "selling sexual services" to aid participant understanding. However, Childlight views the purchase of sexual services from a child as sexual exploitation in all circumstances.

**Figure 6: Odds of online dating frequency by friend engagement in child sexual exploitation material (CSEM)**



## Conclusion and recommendations

This research shows that men with a sexual interest in children, or those who sexually abuse children, are not only more likely to use dating apps than other men, but they also use them more often. Offenders may appear trustworthy, as they are more likely to have a child in their house, work with children, and have a higher education level. However, they are also much more likely to know other offenders, use online privacy tools and cryptocurrency to hide their actions, and engage more frequently with pornography and in online environments where adults and children offer sexual services.

This study highlights that child sex offenders and men with a sexual interest in children are disproportionately active on dating sites, signalling the urgent need for the following key recommendations:

**Recommendation 1.** Improve safeguarding measures on dating platforms. Platforms should implement more substantial user verification processes, such as mandatory ID checks, and develop tools to detect predatory behaviours, such as grooming language or suspicious messaging patterns.

**Recommendation 2.** Conduct targeted user education campaigns. Dating platforms and policymakers should raise single parents' awareness of these risks by providing clear guidance on identifying red flags and protecting their families.

**Recommendation 3.** Improve platform accountability. Dating application platforms should transparently report instances breaking community safety guidelines and further accountability mechanisms such as regulations should be explored.

By prioritising platform accountability, improving user protections, and educating users, we can reduce the risk of single parents being targeted by child sex offenders.

## Limitations

This study has several limitations. Participants were recruited through an online survey panel company, which may affect the generalisability of the findings. Additionally, because the study relies on self-reported data, there is a potential for social desirability bias due to the sensitive nature of the questions. Given the variability in the age of consent across jurisdictions and offence categories, the study defines a child as anyone under 18 when measuring online offending, which may have classified some legal sexual activities as illegal. Nonetheless, survey findings on the prevalence of sexual feelings and behaviours towards children in this study are consistent with those of other studies.

## More information

**Suggested citation:** Salter, M., Tyson, D., Woodlock, D. (2025). Swipe wrong: How sex offenders target single parents on dating apps to exploit their children. In: Searchlight 2025 – Who Benefits? Shining a Light on the Business of Child Sexual Exploitation and Abuse. Edinburgh: Childlight – Global Child Safety Institute

**Researchers:** Professor Michael Salter, Dr Tyson Whitten,
Dr Delanie Woodlock, Mr Matt Tyler, Ms Georgia Naldrett,
Professor Jan Breckenridge, Professor Justine Nolan, Dr Noam Peleg

**Study partners:** Jesuit Social Services

**Registered study protocol:** OSF Registries | The nature of online offending against children: Population-based data from Australia, UK and the USA

**Ethics approval:** University of New South Wales (HC220317)

**Advisory committee members:** Ashley Katz (Director, Child Protection International Partnerships, National Office for Child Safety, Attorney-General's Department), Detective Superintendent Denzil Clark (Operations Coordinator, Queensland Police Service), Mark Dickson (Executive Manager, Financial Crime, Westpac Group), Dr Sarah Napier (Research Manager, OSEC Research Program, Australian Institute of Criminology), Carol Ronken (Director of Research, Bravehearts), Danielle Kelly (Head of Capacity and Prevention, ICMEC Australia)

**Funding acknowledgement:** The research leading to these results has received funding from Westpac as part of the Safer Families, Safer Communities Program. The work of the East Asia and Pacific Hub of Childlight at the University of New South Wales is supported by a collaboration agreement with the University of Edinburgh, under the core grant provided to Childlight – Global Child Safety Institute by the Human Dignity Foundation (grant agreement number [INT21-01]).

For the findings of the Australia report, click here.

# Study E: Hidden casualties of war: CSAM possession during humanitarian crises

## Introduction

In 2024, 72 countries faced humanitarian crises, affecting over 299 million people, including nearly one in five children globally who are living in or fleeing conflict zones (OCHA, 2024). More than 30 million children have been displaced, many of whom are trafficked, abused, or exploited. Two of the United Nations Security Council's six grave violations against children in war include rape and abduction, with girls disproportionately affected by sexual exploitation and boys making up the majority of abductees (UNICEF, 2024a, 2024c).

While sexual violence occurs in all contexts, the risks escalate in humanitarian crises. Armed conflicts, natural disasters, and emergencies create environments in which children are particularly vulnerable to sexual abuse, trafficking and other forms of exploitation (UNICEF, 2024b).

Beyond physical exploitation, children are increasingly at risk online. While sexual violence is often a crime of power, economic incentives now play a significant role. The internet has enabled a growing global market for CSAM, where offenders extort children for explicit content and financial gain (UNICEF, 2024b). Despite extensive research on the impacts of humanitarian crises on children — such as malnutrition, forced conscription and sexual abuse — little is known about the online exploitation and abuse of children during such crises, particularly through CSAM.

CSAM includes images, videos and sound clips documenting the sexual abuse or exploitation of children. Accessing, distributing, or creating CSAM is a crime in most countries, and its ongoing circulation inflicts lasting harm on victims. Given what is known about the heightened risk of exploitation during crises, it is critical to investigate how these risks intersect, particularly in relation to CSAM-sharing and hosting.

Understanding how CSAM circulates during crises is essential for developing effective interventions. This research aims to explore whether humanitarian crises influence the hosting and sharing of CSAM across a variety of environments including peer-to-peer (P2P) networks, which allow users to share files directly without relying on centralised servers. Crises disrupt legal and social systems, creating conditions that facilitate exploitation and abuse. Events like war, migration, and disasters can suspend regulations and weaken protections, leading to increased criminal activity (Spangaro et al., 2013; Marsh et al., 2006).

United Nations (UN) Secretary-General António Guterres has warned that, for traffickers and predators, war is not only a tragedy, but an opportunity, with women and children as primary targets (Guterres, 2022). There is documented evidence of increased trafficking and exploitation of refugees, including in Ukraine, where online searches for explicit content featuring displaced women and children have surged. Analysts warn that traffickers are responding to this demand by coercing refugees into sexual exploitation (The Guardian, 2023). Since the start of the war in Ukraine, over 14.3 million refugees have fled, with family separations at 70%, leaving children at greater risk of abuse and trafficking (Child Helpline International, 2024). Similar patterns exist among Syrian refugees in Turkey, where adolescent girls face exploitation and abuse due to economic desperation, with little publicly available data on technology-facilitated CSEA (ECPAT, 2020).

# Methodology

This study used Child Rescue Coalition (CRC) data to look at the number of IP addresses (unique identifying numbers assigned to devices like phones and laptops) that were in possession of CSAM on P2P networks at various points (intervals) during crises in 20 parts of the world. P2P networks are the various groups of users who agree to share files with one another, there are currently several operating worldwide.

Countries/places which were undergoing humanitarian crises were identified from ReliefWeb and UN Refugees, which list emergencies and crises. From these sources, dates of the beginning of the crises were identified. For example, the conflict start in Ukraine is officially listed as 24 February 2022 (UNHCR, 2025). The intervals of data for each country were the past 90 days from the start of the crisis; the past 90 days from 15 October 2024 (the date when the data was collected); and a central date between the date of crisis start and 15 October 2024.

The places examined were Ukraine, the Holy Land, Sudan, Yemen, Afghanistan, Syria, Ethiopia, Myanmar, Venezuela, Sierra Leone, Central African Republic, Mauritania, Chad, Benin, Ghana, Togo, Cote d'Ivoire, Iraq, Somalia and South Sudan. In each of these places, it was decided to measure the number of IPs in possession of CSAM three months prior to the crisis, at a point during the crisis, and with a final measurement representing the current number of users as all the crises were ongoing. This data was then compared with available and applicable country-level data from both the Association of Internet Hotline Providers (INHOPE) and the National Center for Missing and Exploited Children (NCMEC), which produce metrics on the number of reported CSAM and CSAM hosted in some of the same countries.

Reports of child sexual abuse material (CSAM) hosting rose in Ukraine and the Holy Land,[3] while peer-to-peer sharing of CSAM fell in war, famine and disease settings.

# Key findings

## Conflict and war

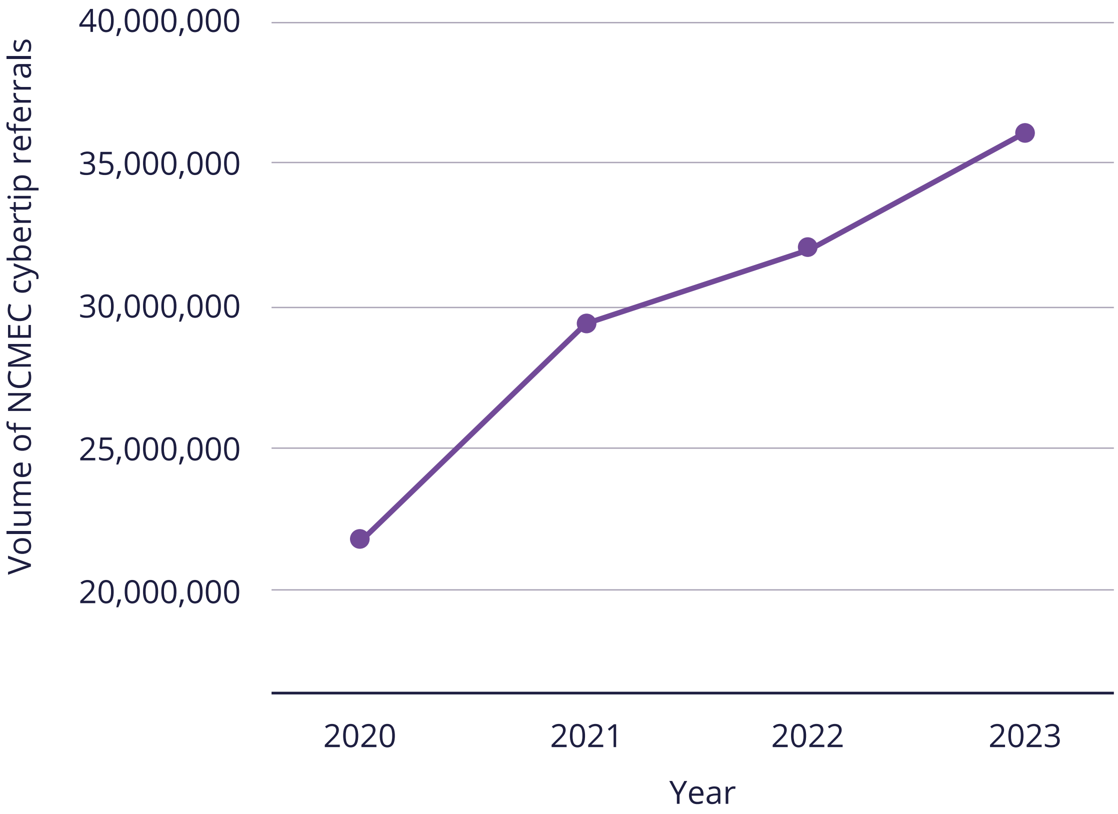
Countries experiencing a period of recognised conflict, whether internal or external, including Ukraine, the Holy Land, Sudan, Yemen, Myanmar, Venezuela, Central African Republic and Iraq, had the highest number of IP addresses linked to CSAM possession among all crisis types analysed. Notably, Venezuela had the largest number of IP addresses in possession of CSAM prior to the onset of the conflict. This data is important in order to understand the trends, as Venezuela's crisis began around 2016, approximately six years earlier than Ukraine's in 2022, during a period when P2P networks were more commonly used. Additionally, Venezuela's conflict coincided with the ratification of the United Nations Convention on the Rights of the Child, providing a critical reference point for the country's evolving crisis.

In terms of P2P CSAM-sharing, three places (Venezuela, Ukraine, and the Holy Land) showed a reduction of over 1,000 IP addresses possessing such material across the three measured intervals. Venezuela experienced the largest drop in IP addresses, particularly in the first measured interval. On average, there was a 31% decrease in IP possessing CSAM across all countries and at all crisis intervals. This could also point to conflict displacing people away from the countries and regions, which would lead to CSAM possession in other locations away from the conflict.

[3] The Holy Land encompasses Israel and Palestine, including the Gaza strip.

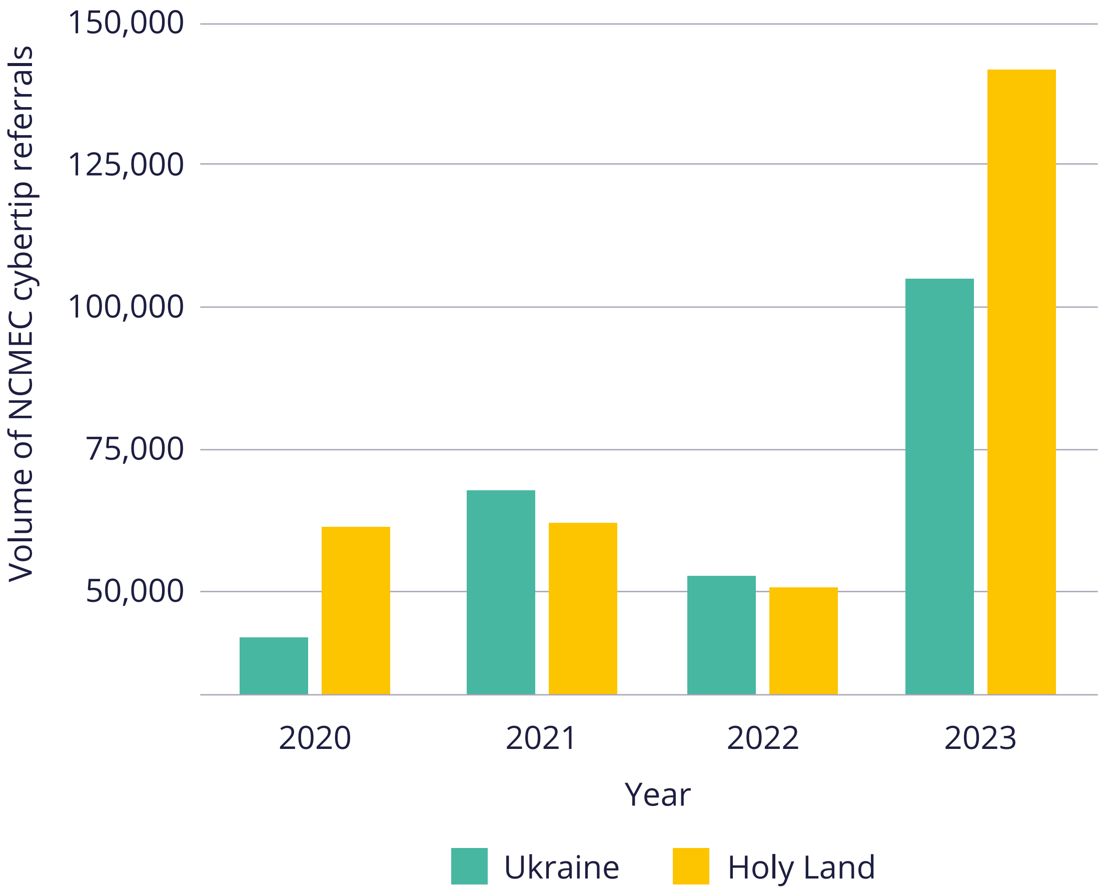
However, despite the decline in P2P CSAM-sharing, reports of CSAM to organisations such as the NCMEC and INHOPE registered a sharp increase during these conflicts. For example, NCMEC data revealed that the number of CSAM reports surged in some countries (by **over 150%** in Ukraine and the Holy Land), despite the decrease in P2P activity. Although it is important to note that NCMEC referrals have been increasing year on year globally (Figure 1), we see some conflict related fluctuations in NCMEC data on CSAM due to conflict for both Ukraine and the Holy Land (Figure 2). This discrepancy highlights the complex relationship between P2P-sharing and formal reporting mechanisms, where increased awareness, reporting channels, and law enforcement attention may be influencing the rise in official reports, even as P2P activity decreases. The data may also reflect a shift in sharing CSAM away from P2P.

### Figure 1: Volume of NCMEC cybertip referrals on CSAM globally, 2020–2023



Sources: NCMEC Cybertipline Country reports 2020 - 2023 (NCMEC, 2023)

**Figure 2: Volume of NCMEC cybertip referrals on CSAM for the Holy Land and Ukraine, 2020–2023**



Sources: NCMEC Cybertipline Country reports 2020 - 2023 (NCMEC, 2023)

It is also important to note that, while conflict/war was considered the primary crisis in these countries, other aspects, such as famine, political instability, or economic collapse, could have been happening concurrently, potentially influencing the findings. These multifaceted challenges create a more complex environment that can exacerbate the risks faced by children and increase the opportunities for CSAM-sharing.

One notable P2P-sharing exception was Iraq, where the number of IP addresses linked to CSAM possession increased from zero to 90 during the period of conflict. This was the largest increase observed across all the countries in the study. Interestingly, NCMEC reported a decrease in the number of CSAM-related reports from Iraq during the same period, suggesting a possible shift toward more P2P sharing, for which formal reporting may not fully capture the extent of the issue. Table 1 outlines the data sources for the countries affected by conflict/war examined in this study.

### Table 1: Changes in volume of reports, hosting notices and IPs linked to possession of CSAM in places with war/conflict

| Country and start date of crisis | Type of first recorded crisis | NCMEC data: volume of reports and percent change (2020–2023) | Hotlines hosting data: volume of hosting notices and percent change (2020–2024) | P2P file sharing data: volume of IPs and percent change (start date – Oct 2024) |
|---|---|---|---|---|
| **Ukraine**<br>(August 2021) | War/ conflict | +62,213<br>(+250%) | +10,652<br>(+63%) | -1,233<br>(-47 %) |
| **Holy Land**<br>(Israel and Palestinian territory) (April 2023) | War/ conflict | +80,031<br>(+230%) | +2<br>(+200%) | -1,049<br>(-39%) |
| **Venezuela**<br>(December 2014) | War/ conflict | +115,592<br>(+195%) | +1<br>(+100%) | -69,799<br>(-98%) |
| **Sudan**<br>(October 2022) | War/ conflict | -45,773<br>(-55%) | No data | -23<br>(-88%) |
| **Myanmar**<br>(February 2017) | War/ conflict | -109,759<br>(-65%) | No data | -34<br>(-79%) |
| **Central African Republic** (June 2020) | War/ conflict | -19<br>(-6%) | No data | None |
| **Yemen**<br>(September 2016) | War/ conflict | -568<br>(-93%) | No data | +251,201<br>(+460%) |
| **Iraq**<br>(October 2017) | War/ conflict | -176,220<br>(-81%) | No data | +90<br>(+9,000%) |

Sources: Childlight analysis of CRC data; and NCMEC Cybertipline Country reports 2020–2023 (NCMEC, 2023)

## Famine and natural disasters

The following five countries — Afghanistan, Ethiopia, Sierra Leone, Somalia, and South Sudan — were categorised under natural disaster crises. Natural disasters are defined as hurricanes, floods, cyclones, earthquakes and other weather or geological-related crises. The highest number of IP addresses in possession of CSAM across this group of countries was four IP addresses, which were recorded in both Ethiopia and Afghanistan at the start of the crisis. Both of these countries also saw an increase in the number of IPs possessing CSAM during the measured intervals. The other three countries in this group — Sierra Leone, Somalia, and South Sudan — reported either one or zero IP addresses during the measured periods, suggesting that very few people in these regions were using P2P networks for sharing CSAM.

It is important to note that the recorded date of October 2024 represents the most recent data, and the highest number of IPs linked to P2P sharing observed was from the start of the respective crises. This relatively low number of IP addresses in possession of CSAM in countries experiencing famine and natural disasters, compared to those in conflict zones, could be attributed to several factors. It should also be noted that the overall numbers for peer-to-peer users in possession of CSAM are low and should be interpreted with caution. For instance, limited access to technology and internet connectivity in some of these places may have contributed to fewer opportunities for individuals to engage in P2P file sharing. In many cases, P2P networks are dependent on widespread internet access and sufficient infrastructure, which may be lacking or severely affected in countries facing significant humanitarian crises, including those facing famine or natural disasters.

Additionally, famine or natural disasters may not create the same conditions for the exploitation of children online as armed conflict does. War and conflict often lead to rapid breakdowns in social and legal systems, creating environments where children are more vulnerable to exploitation, including through P2P networks. In contrast, although famine and natural disasters certainly disrupt societies, they might not present the same immediate risks for technology-facilitated child sexual exploitation and abuse (TF-CSEA). While CSAM possession on peer-to-peer networks may be limited in these countries, when looking at report-related data from NCMEC, three of the five saw an increase in reporting of CSAM. One country, Somalia, saw little change over time in NCMEC reports, while Ethiopia saw their reports reduce by approximately half.

Nevertheless, the data from these countries should be interpreted with caution. The lower prevalence of CSAM-sharing in these regions may not necessarily reflect the full scope of the issue. For example, underreporting or limited data availability could result in an incomplete picture of the online exploitation of children during these crises. Further research is needed to explore how factors such as cultural attitudes, limited access to reporting mechanisms, and low internet penetration may contribute to the disparity observed in the data.

### Table 2: Changes in volume of reports, hosting notices and IPs linked to possession of CSAM in places with famine and natural disasters

| Country and start date of crisis | Type of crisis | NCMEC data: volume of reports and percent change (2020–2023) | P2P file sharing data: volume of IPs and percent change (start date – Oct 2024) |
|---|---|---|---|
| **Afghanistan**<br>(January 2015) | Famine and natural disaster | +81,789<br>(+170%) | +4<br>(+33%) |
| **Ethiopia**<br>(November 2020) | Famine and natural disaster | -8,104<br>(-46%) | +4<br>(+300%) |
| **Sierra Leone**<br>(November 2018) | Famine and natural disaster | +289<br>(+130%) | None |
| **Somalia**<br>(January 2015) | Famine and natural disaster | -794<br>(-4%) | +1<br>(+100%) |
| **South Sudan**<br>(March 2017) | Famine and natural disaster | +1,009<br>(+157%) | None |

Sources: Childlight analysis of CRC data; and NCMEC Cybertipline Country reports 2020–2023 (NCMEC, 2023)

# Conclusion

The findings of this study provide an exploratory and nuanced understanding of the nature and prevalence of CSAM in humanitarian contexts, revealing potential trends in different types of crises. The data highlights that conflict and war zones exhibit the highest rates of CSAM-sharing. Ukraine, the Holy Land and Venezuela show a substantial number of IP addresses linked to CSAM possession, as well as a sharp rise in reports of CSAM hosting or uploads. This trend could be largely driven by the breakdown of social and legal systems, displacement and the resulting risks for children in conflict areas. The continued sharing of CSAM in these places, despite overall reductions in P2P network activity, underscores the persistent and evolving risk of TF-CSEA during crises.

Conversely, countries experiencing famine and natural disasters tend to report lower rates of CSAM possession compared to conflict and war zones. While these regions may still face significant risks, the data shows a relatively smaller presence of CSAM on P2P networks. The lower levels of CSAM sharing in these contexts could be attributed to factors such as limited internet connectivity, lower penetration of P2P technologies and perhaps a reduced focus on technology-facilitated child sexual exploitation and abuse during these crises.

The decline in CSAM activity over time in several countries, including those impacted by conflict, suggests that interventions and restrictions on P2P networks may have had an effect, although further research is needed to confirm this. While the data points to a decrease in IPs sharing CSAM across P2P in the studied countries, NCMEC global data continues to show an increase in the numbers of CSAM reports globally, most recently passing 36 million reports (NCMEC, 2024). This suggests that CSAM sharing and uploads are occurring in these countries/regions outside of peer-peer networks.

Nevertheless, some hotspots warrant more focused monitoring. Countries in active conflict zones, especially those with significant displacement of populations, remain high-risk areas for both contact and TF-CSEA. The data shows a potential rise in demand for CSAM linked to displaced populations, such as in Ukraine, where a marked increase in the exploitation and abuse of at-risk children online has been observed. Furthermore, the findings from Iraq, which saw a sudden spike in CSAM possession during the conflict, suggest the need for heightened vigilance in such contexts, where internet accessibility and the digital footprint may evolve rapidly.

Caveats regarding the data sources are essential for interpreting these findings. The numbers presented rely on data from P2P networks, for which the number of IP addresses linked to CSAM may not accurately reflect the full scope of the issue. For example, an individual user possessing multiple files could be counted as a single IP address, which can distort the overall picture. Additionally, variations in internet connectivity, the availability of technology and the degree of law enforcement oversight in different regions significantly influence the presence and distribution of CSAM. The study's focus on P2P CSAM data also means that the true volume of CSAM — both in terms of files shared and victims depicted — remains difficult to quantify and separate. The INHOPE and NCMEC data on hosting of CSAM, as well as reports of CSAM, help to unveil the potential volume of files. In bringing together all three of the available data sources, this study begins to explore how CSAM sharing migrates between technology facilitated spaces, both within countries and across the globe. These limitations underscore the need for further research and more comprehensive data sources to capture the full scale of TF-CSEA in humanitarian crises.

In conclusion, while the research has revealed key trends in the sharing of CSAM during periods of humanitarian crisis, it also highlights the complexities and challenges of monitoring this issue effectively. Ongoing data collection, improved reporting mechanisms and a coordinated international effort are crucial to mitigate the risks of TF-CSEA and to protect vulnerable children in these increasingly complex environments.

# Recommendations

The following recommendations have been tailored to specific phases of crises (pre-crisis, during crisis response, and post-crisis).

## Pre-crisis phase

**Recommendation 1.** Improve awareness and training for humanitarian actors. It is essential to conduct regular, targeted awareness programmes for humanitarian actors (NGOs, frontline responders, etc.) on the nature of TF-CSEA, the mechanisms for detecting it, and the importance of safeguarding children from online and offline exploitation and abuse.

**Recommendation 2.** Ensure that TF-CSEA is explicitly included in the child protection rapid assessments conducted in the immediate aftermath of a crisis, particularly in conflict zones, refugee camps, and areas with high displacement. This could help identify regions at high risk of exploitation.

**Recommendation 3.** Many affected communities may have weak legal frameworks for protecting children, particularly regarding online exploitation. It is important to collaborate with governments and local actors to strengthen laws and community-based child protection systems that prevent TF-CSEA.

## During crisis response phase

**Recommendation 4.** Implement immediate child protection protocols in refugee camps. During emergency response, child protection measures need to address both immediate physical threats (such as trafficking and abduction) and digital risks (such as TF-CSEA). Ensure that child protection services in refugee camps and displacement settings are prepared to address both forms of abuse.

**Recommendation 5.** Increase data collection on TF-CSEA. As humanitarian crises disrupt traditional social and legal systems, tracking TF-CSEA becomes increasingly important. More comprehensive data collection mechanisms should be put in place to track incidents of online abuse and exploitation during crises.

## Post-crisis phase

**Recommendation 6.** Strengthen digital literacy and resilience for children and communities. After the crisis, as children and families begin to rebuild, it is crucial to enhance their digital literacy and resilience to TF-CSEA. This includes providing information to children, parents, teachers and others about the risks of online platforms and the importance of online safety.

**Recommendation 7.** Monitor and evaluate TF-CSEA prevention efforts. Following the resolution of immediate humanitarian needs, long-term monitoring of the effectiveness of interventions to prevent TF-CSEA is essential. This ensures that policies and programmes are continuously adapted and improved based on real-world data and outcomes.

## Overarching Recommendation

This research is a nascent step in a wider study, also examining refugee crises and Covid-19. Further research is required to compare activities before, during and after the crises. Further research is also required into the number of victims portrayed in CSAM exchanged on P2P in relation to the number of IPs showing they are in possession of these files. This will provide a better understanding of the impact of one single user exchanging CSAM on this network and the scope of the harm this can cause.

# Limitations

As P2P networks require many users to possess and share the same files in order to facilitate quick and efficient transfer, those using the network are encouraged to make all their files publicly available. As such, while it is in the interest of the network for users to share that they are in possession of files, including CSAM, some users may choose not to share these files for fear of detection. Hence, the data may present an inaccurate representation of the number of users engaging in P2P networks for the purpose of the proliferation of CSAM.

As noted above, the numbers also do not represent a 1:1 ratio of IPs to users or IPs to the number of victims portrayed in the sexual abuse material. Further study is needed concerning the computer storage space required for each file, along with content based on analysis of the files, to get a sense of the amount of CSAM contained.

The findings are also limited by the available data, which meant that certain crises were not included, having begun before 2014 and, therefore, would not be fully represented in the ten-year period of available data. This was further complicated by limitations around the geolocation of the IPs, which had varying degrees of specificity with certain countries/regions, such as the Holy Land in particular, being grouped.

The crisis types were not experienced in isolation, with many of the countries experiencing more than one crisis type during the studied period. The countries were organised by the first listed crisis type, which may have influenced the findings. Many of the countries were likely to have been simultaneously impacted by increased globalisation and internet connectivity as well.

While data was collected prior to the onset of the crisis, at a midpoint and at the end, this is only within country data and does not include a control group. Evidence suggests that the trends presented here may mimic larger global trends (NCMEC data increasing year on year; P2P data decreasing), but this needs to be explored more in depth as certain country variations exist. We also know that TF-CSEA is a transnational phenomenon; CSAM may be produced on children in humanitarian crises, hosted in a second country and consumed by an offender in a third country. Thus, this data is very likely an underestimate of the true scale of the issue. More research is needed to better understand the demand-side of distribution and consumption of CSAM during humanitarian crises.

## More information

**Suggested citation:** McFeeters, A., Page, S., Stevenson, J., & Fry, D. (2025). Hidden casualties of war: CSAM possession during humanitarian crises. In: Searchlight 2025 – Who Benefits? Shining a Light on the Business of Child Sexual Exploitation and Abuse. Edinburgh: Childlight – Global Child Safety Institute.

**Researchers:** Dr Ashleigh McFeeters, Ms Sabrina Page (PhD Can.), Mr James Stevenson, Professor Deborah Fry

**Study partners:** Child Rescue Coalition

**Registered study protocol:** OSF Registries | CSAM Content P2P Networks CRC

**Ethics approval:** University of Edinburgh, Childlight Research Ethics Sub-Committee (UTGNO-AMF-0050424CL)

**Advisory committee members:** Liz Wright (INTERPOL), Eleena Ahmed (UK Foreign, Commonwealth & Development Office), Elly Hanson (clinical psychologist), Rosalind Willi (SOS Children's Villages), Nigel Jenkins (former board member Médecins Sans Frontières [MSF] Amsterdam, retired)

**Funding acknowledgement:** The research leading to these results has received funding from the Human Dignity Foundation under the core grant provided to Childlight – Global Child Safety Institute under the grant agreement number [INT21-01].

# PART 3. ACCOUNTABILITY

This section examines the effectiveness of legal and regulatory frameworks in holding perpetrators and systems accountable for child sexual exploitation and abuse (CSEA). Laws and enforcement mechanisms often struggle to keep pace with evolving threats, leaving critical gaps that allow offenders to evade justice. Through case studies from five nations, we assess where current legislation succeeds, where it fails, and what must change — particularly in addressing AI-generated child sexual abuse material (CSAM). We also explore how policymakers can close loopholes, strengthen enforcement and ensure justice systems are equipped to respond effectively to emerging forms of exploitation.

# Study F: Legal challenges in tackling AI-generated CSAM across the UK, USA, Canada, Australia and New Zealand: Who is accountable according to the law?

## Introduction

This study is among the first to examine the regulatory context of five closely inter-connected countries (UK, USA, Canada, Australia and New Zealand) in terms of accountability around child sexual abuse material (CSAM) created via generative artificial intelligence (gen-AI). The findings of our legislative review have helped us identify the key strengths as well as weaknesses of the legislative contexts studied. These countries were selected due to their democratic political systems, technological advances and progressive legislative systems. We examined 29 pieces of legislation and 25 cases for the UK context; 27 pieces of legislation in Australia and New Zealand, together with 4 emerging cases; as well as 279 statutes, 52 pieces of pending legislation and 65 cases in the US and Canada.

## Methodology

Legislation and case law in five countries was reviewed and analysed, informed by the 'black-letter law' approach, also known as the doctrinal legal research method. This approach focuses on the letter, rather than the spirit, of the law, looking primarily at what the law says and at well-established legal principles, and less at the social context or implications for policymaking.

Existing laws provide good grounds for accountability, but there are still notable gaps. These gaps need to be addressed in order to fully provide the protections and accountability needed to keep children safe in view of the advent of AI. Significant legal reforms are underway in all jurisdictions examined.

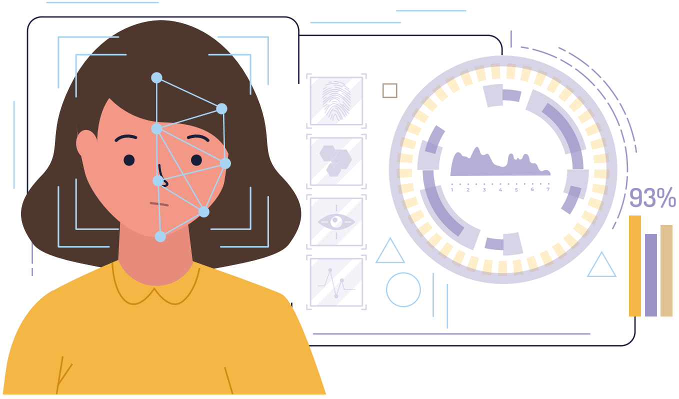
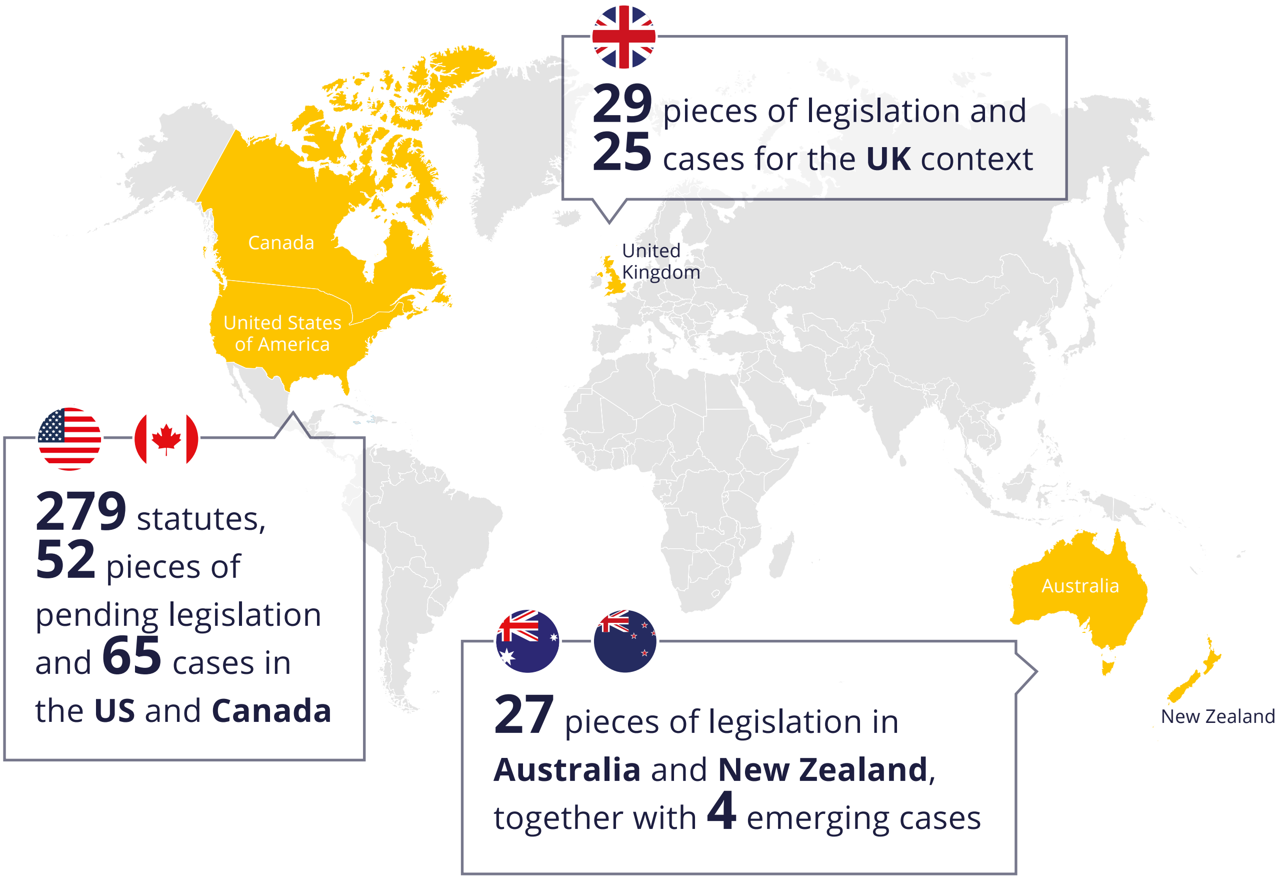


**Figure 1: The number of legislation and cases reviewed for this study**



**29** pieces of legislation and **25** cases for the **UK** context

**279** statutes, **52** pieces of pending legislation and **65** cases in the **US** and **Canada**

**27** pieces of legislation in **Australia** and **New Zealand**, together with **4** emerging cases

# Findings

Legislation in the UK is divided between reserved and devolved matters. Reserved legislation is adopted by the Westminster Parliament. Devolved legislation is the legislation adopted by the Scottish Parliament or the Northern Ireland Assembly. Both levels of legislation were examined for this study covering all 4 nations of the UK (England, Northern Ireland, Scotland and Wales).

The legislation that is relevant for cases of AI-generated CSAM focuses on two types of indecent images. One type is indecent pseudo-photographs, meaning photographs as well as videos and films made by computer graphics that have a photo-realistic appearance, i.e., they look real. The other type covers prohibited pseudo-images that do not look realistic, such as drawings and cartoons or hentai and manga. Manga are Japanese comic books and graphic novels, while hentai are a type of Japanese manga and anime that portrays sexualised content, storylines and characters. There is concern in some parts of the world, such as the UK, that when these types of imagery present children in a pornographic, offensive or otherwise obscene way, focus on children's private parts or display prohibited acts including children, there is a risk that they may be normalising child abuse and encouraging harmful behaviour. Notably, these concerns are not shared on a global scale and research on the matter is not yet robust.

We found that there is good coverage around a series of offences with regards to pseudo-photographs, i.e., the acts of making, taking, possessing and disseminating pseudo-photographs are all covered, irrespective of the technology used, thus covering cases of generative AI or deepfakes. This is evidenced by the first emerging case in England, where an offender who created CSAM using generative AI was arrested, charged and sentenced to 18 years in prison. In this instance, and as per a recent BBC report, the Crown Prosecution Service, warned that those thinking of using AI "in the worst possible way" should be "aware that the law applies equally to real indecent photographs and AI or computer-generated images of children" (Gawne, 2024). That said, the law is silent on whether the criminalisation of indecent pseudo-photographs of children extends in cases of both real/identifiable and fictitious children.

However, this protection tends to be less efficient with regards to non-realistic images, including cartoons, manga and drawings. While possession and dissemination are criminalised, the act of making such imagery is not criminalised in England and Wales. The largest gap in protection with regards to the above imagery exists in Scotland, as the making and possession of indecent non-realistic images in Scotland is not criminalised. The nation that seems to have the most robust legislative framework against all acts related to indecent non-realistic images is Northern Ireland.

Another gap that exists across the UK is around the possession of paedophile manuals, meaning guides on how to sexually abuse children. Existing legislation does not apply in cases of possessing a paedophile manual that specifically instructs on how to misuse generative AI to produce CSAM. Ongoing UK legal reforms are targeting this specific gap in the legislation (Home Office, 2025). In Scotland, no legislation on paedophile manuals exists whatsoever. Arguably, this may heighten the risk of widespread dissemination of manuals containing instructions on how to sexually abuse and/or exploit children.

There has been no case law, i.e., court cases, on criminal liability for omissions (the failure to perform a legal duty when one can do so) in cases of AI-generated CSAM, but there may be room to argue that it is possible for such liability to arise in the case of a close personal relationship and assumed responsibilities, i.e., in relation to a child's parent(s) or guardian(s).

Notably, the UK recently adopted the Online Safety Act, which places new duties on social media companies and search service providers to protect children and other vulnerable adult users online. The Act applies specifically to user-to-user services (e.g. social media, photo or video-sharing services, chat services and online or mobile gaming services); search services; and to businesses that publish or display pornographic content (OFCOM, 2025). The regulation of content that is harmful to children is a top priority for the Online Safety Act. Therefore, and among other legislated duties, the law mandates the above-mentioned companies to remove illegal content, such as CSAM, and, even if this has been created by generative AI, take steps to prevent users from encountering it (OFCOM, 2024).

From a civil perspective, there is no specific legislation or case law in the UK that directly addresses this issue, leaving a significant gap. However, AI-generated CSAM seems to fall under the protective remit of the Data Protection Act 2018.

There is the ability to claim compensation in the UK with regards to CSAM created via gen-AI technologies that includes figures modelled after real, identifiable children via a number of pathways (a civil claim, privacy infringement, compensation order via criminal courts, and, much less likely, via the Criminal Injuries Compensation Scheme [CICA]). However, the liability for AI-CSAM, i.e., the question 'who is the author of AI', remains currently unclear under existing legislation across the UK.

What also became evident from the above analysis is the fact that the UK lacks a targeted AI industry regulation, like the one that was recently adopted in the European Union in the form of the EU's AI Act. There seem to be no plans at the moment for a standalone UK AI Act.

Lastly, a more recent legal reform concerns AI tools. More specifically, the UK is considering making it illegal to possess, create or distribute AI tools designed to create CSAM, with a punishment of up to five years in prison (Home Office, 2025).

# Recommendations

Based on these findings, the following recommendations are made for the UK:

**Recommendation 1.** Update the law to clearly criminalise all acts relevant to pseudo-photographs that depict purely fictitious children, i.e., making, taking, disseminating and possessing such material.

**Recommendation 2.** The Scottish Government should introduce legislation to criminalise all acts relevant to non-photographic indecent images of children, i.e., making, taking, disseminating and possessing such material.

**Recommendation 3.** Criminalise the making of prohibited non-photographic images of children.

**Recommendation 4.** Update UK legislation on paedophile manuals to make them applicable to pseudo-photographs. As stated above, reforms on the matter are currently underway.

**Recommendation 5.** Introduce Scottish legislation criminalising paedophile manuals.

## Australia and New Zealand

# Findings

With regards to Australia, the same issues were examined on both a national as well as a state and territory level, whereas in New Zealand they were examined only on the national level, as no relevant legislation exists on a devolved basis. It is worth considering that Australia also enacted an Online Safety Act (OSA) in 2021, which imposes certain duties on online service providers with regard to protecting Australians, in particular children and vulnerable adult users online.

The eSafety Commissioner was established in 2015 (then the 'Office of the Children's eSafety Commissioner') in Australia and serves as an independent regulator for online safety, with powers to require the removal of unlawful and seriously harmful material, implement systemic regulatory schemes and educate people around online safety risks.  Under the OSA, there are currently enforceable codes and standards in force which apply to AI-generated CSAM with civil penalties for services that fail to comply. In particular the 'Designated Internet Service' Standard applies to generative AI services, as well as model distribution services.

The OSA was independently reviewed in 2024. The Review examined the operation and effectiveness of the Act and considered whether additional protections are needed to combat online harms, including those posed by emerging technologies (Minister for Communications, 2025). The Final Report of the review was tabled in Parliament in February 2025.

The Australian Government has also recently conducted consultations regarding the introduction of mandatory guardrails for AI in high-risk settings, which considers guardrails like ensuring that generative AI training data does not contain CSAM (Australian Government, Department of Industry, Science & Resources, 2024).
No such legislation exists in New Zealand, although there are ongoing discussions and legal reform suggestions around the potential introduction of similar legislation there.

In both Australia and New Zealand, existing definitions of CSAM or similar terminology used in criminal legislation are broad enough to capture AI-generated CSAM. As a result, and despite limited case law on the matter due to the emerging character of gen-AI technologies, sentencing decisions have emerged in the Australian states of Victoria and Tasmania involving offenders who produced gen-AI CSAM.

In New Zealand, no cases have yet been identified in which offenders have been sentenced for offences involving AI-generated CSAM, however, press reports suggest that offenders have been charged in relation to such material. In addition, there are reports of the New Zealand customs service seizing gen-AI CSAM, suggesting that they consider that they have the jurisdiction to do so. No cases have been identified in Australia or New Zealand in which AI software creators or holders of datasets used to train AI have been considered criminally liable in relation to the production of CSAM using their platforms or any other such charges.

In New Zealand, certain pieces of legislation (e.g., Crimes Act 1961 and Harmful Digital Communications Act 2015) do not appear to apply in cases of gen-AI CSAM that portrays purely fictitious children. This is to an extent expected, as both laws require harm to be inflicted upon an identifiable natural person and this is not the case in instances of AI-generated CSAM containing purely fictitious children.

In both Australia and New Zealand, there are no pending reforms to expand criminal accountability in relation to gen-AI CSAM to AI software creators and dataset holders. Given that the definitions of CSAM in existing criminal legislation appear broad enough to capture AI-generated material, this is not surprising.

# Recommendations

Based on these findings, the following recommendations are made for Australia and New Zealand:

**Recommendation 1.** Monitor the applicability of relevant legislation (particularly of the Australian Online Safety Act) as was recently done by the review of the OSA and the Australian Government's intention to introduce a digital duty of care, and review emerging case law to further assess applicability.

**Recommendation 2.** Policymakers and legislators need to thoroughly assess whether civil penalty provisions should be further increased in Australia and New Zealand, in line with other jurisdictions internationally.

**Recommendation 3.** Policymakers and legislators need to thoroughly assess whether existing regulations cover criminal liability for AI software creators or dataset holders who failed to install proper guardrails in their products that would safeguard children before rolling them out in the market. We found no specific legislation on this. Case law interpretation on this is also crucial. These topics also relate to questions around who the author of AI is and if the law should delineate a minimum standard of guardrails that need to be met by AI creators, beyond which they have no liability.

## United States of America and Canada

# Findings for the USA

In the United States of America, the regulatory framework consists of federal laws and state-based laws. Federal CSAM statutes, together with case law, criminalise several categories of harmful material. Still, a significant number of vague points persist. Federal laws are relatively robust, but there is a gap with regards to the criminalisation of artificial CSAM that depicts purely fictitious children. Civil remedies, although significant, are limited in scope. Copyright and consumer protection laws offer some avenues for redress, but they are also limited.

Prosecutors typically require concrete evidence to prosecute, such as incriminating communication or attempts to sell or trade material. These are often hard to obtain. This challenge is increased by more advanced AI models that generate hyper-realistic CSAM without training on authentic abuse imagery. This means that even if we start regulating how AI models are trained, these advanced AI models that can create realistic CSAM without the need for training will be evading regulation.

Drawing on copyright law, platforms and developers can be held liable if they knowingly contribute to the sharing of harmful content. However, online platforms are protected from civil liability for user-generated content, complicating efforts to hold them accountable for hosting AI-generated CSAM. Despite efforts to change the law on this, balancing platform liability with the protection of free speech is a major challenge.

The legal landscape is even more fragmented on a state level due to several outdated pieces of legislation around so-called 'child pornography',[4] which fail to address newer forms of technology-facilitated child sexual abuse. State-level civil remedies are often inadequate, leaving gaps in accountability for users, developers, distributors and third-party beneficiaries.

On 16 April 2024, the Child Exploitation and Artificial Intelligence Expert Commission Act of 2024 was introduced to address the creation of CSAM using AI. This legislation provides for the establishment of a commission to develop a legal framework that will assist law enforcement in preventing, detecting and prosecuting AI-generated crimes against children.

## Findings for Canada

In Canada, there is a distinction between federal law and province-based law. The federal Criminal Code lacks specific prohibitions against AI-generated CSAM. Still, the relevant sections of the Canadian Criminal Code have been interpreted widely by the Supreme Court of Canada to provide coverage for several types of harmful material. There remain two exceptions, though. The first is for material that has been created only for personal use and the second is for works of art that lack intent to exploit children. Canadian federal law criminalises the non-consensual distribution of intimate images. However, whether these provisions apply to AI-generated CSAM is uncertain. Enforcement is the responsibility of provincial agencies, and civil remedies for victims vary widely across provinces, creating a patchwork of protections in which access to relief depends on the victim's location.

Privacy laws in Canada offer some avenues for assistance, but they lack a more tailored character to address the specific harms associated with AI-generated CSAM. Copyright law offers a potential, although complex, avenue for addressing AI-generated CSAM.

[4] Childlight follows the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. The terms 'child abuse', 'child prostitution', 'child pornography' and 'rape' are used in legal contexts.

Lastly, in Canada, a significant law reform that was proposed is the Online Harms Act. If passed, this Act will create a new regulatory framework requiring online platforms to act responsibly to prevent and mitigate the risk of harm to children on their platforms. Under the Act, online platforms would have a duty to implement age-appropriate design features and to make content that sexually victimises a child or re-victimises a survivor inaccessible, including via the use of technology, to prevent CSAM from being uploaded in the first instance. A new Digital Safety Commission would oversee compliance and be charged with the authority to penalise online platforms that fail to act responsibly.

Accordingly, the Act would create a legally binding framework for safe and responsible AI development and deployment that could potentially apply to restrict or penalise content that would otherwise be legal, but that poses a substantial risk of sexual exploitation or revictimisation of a child. Prorogation of the Parliament of Canada ends the current parliamentary session. As a result, all proceedings before Parliament end, and bills that have not received Royal Assent are 'entirely terminated'. This means that the Online Harms Act would need to be reintroduced by the new government in Canada before it could be considered again for Royal Assent (Lexology, 2025).

## Recommendations

Based on these findings, the following recommendations are made for the USA and Canada:

**Recommendation 1.** Amend existing CSAM laws to explicitly cover AI-generated content, even when it includes fictitious children.

**Recommendation 2.** Amend CSAM laws to regulate the misuse of AI.

**Recommendation 3.** Amend CSAM laws to cover content that is legal, but poses a substantial risk of harm to minors (e.g., grooming or nudity content).

**Recommendation 4.** Establish a legally binding framework for safe and responsible AI development and deployment.

**Recommendation 5.** Expand legal protections to include control over one's own image.

## Limitations

The main limitation of this research stems from the emerging character of the technology it considers. This applies particularly to case law and the interpretation of existing legislation by courts, because, due to the developing character of this technology, we still have not seen robust case law established in relation to AI and deepfake CSAM that would create strong precedents. As such, this research should be replicated in 5 to 10 years' time, when there is more robust case law on the matter.

## More information

**Suggested citation:** Gaitis, K.K., Fakonti, C., Lonard, Z., Lu, M., Schidlow, J., Stevenson, J., & Fry, D. (2025). Legal challenges in tackling AI-generated CSAM across the UK, USA, Canada, Australia and New Zealand: Who is accountable according to the law? In: Searchlight 2025 – Who Benefits? Shining a Light on the Business of Child Sexual Exploitation and Abuse. Edinburgh: Childlight – Global Child Safety Institute

**Researchers:** Dr Konstantinos Kosmas Gaitis, Dr Chrystala Fakonti, Ms Zoe Lonard, Dr Mengyao Lu, Ms Jessica Schidlow, Mr James Stevenson, Professor Deborah Fry

**Study partners:** Child USA, Norton Rose Fulbright Australia and Glasgow Caledonian University

**Registered study protocol:** OSF Registries | Does existing legislation on CSEA/CSAM across the Five Eyes nations allow for criminal liability or any other form of accountability with regards to AI-generated CSAM

**Ethics approval:** University of Edinburgh, Childlight Research Ethics Sub-Committee (DELOC-KKG-0030424CL)

**Advisory committee members:** Professor Ben Mathews (School of Law, Queensland University of Technology), Dan Sexton (Chief Technology Officer, Internet Watch Foundation), Michael Skwarek (Manager, Codes and Standards Class 1, Industry Compliance and Enforcement, Australian eSafety Commissioner)

**Funding acknowledgement:** The research leading to these results has received funding from the Human Dignity Foundation under the core grant provided to Childlight – Global Child Safety Institute under the grant agreement number [INT21-01].

# Study G: Unmasking exploitation: Study of Supreme Court cases reveals changing landscape of CSEA in the Philippines

## Introduction

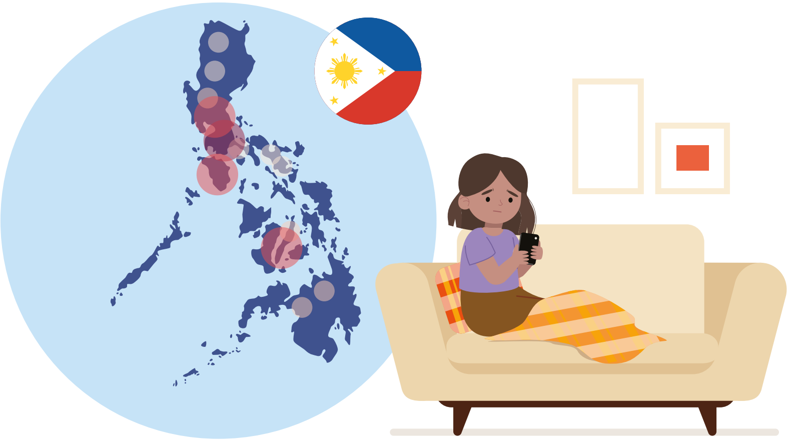
This study examines the evolution of commercial sexual exploitation of children (CSEC) in the Philippines, focusing on cases from 2003 to 2024, particularly those heard by the Supreme Court. The implementation of the Anti-Trafficking in Persons Act (Republic Act 9208) in 2003 established legal frameworks to combat trafficking and exploitation. Analysing 56 Supreme Court cases, the study highlights how exploitation methods have evolved, becoming more difficult for authorities to detect and prevent. The findings emphasise the increasing complexity of both online and offline exploitation, stressing the need for stronger legal and social protections for children.

Previously, large, organised syndicates controlled many victims, but now smaller, more covert groups exploit children. These groups are harder to detect as they use discreet methods and exploitation is increasingly occurring within families and close social circles. The locations of abuse have shifted from public venues to private homes and online platforms, where abuse can be livestreamed or recorded. Recruitment tactics have also evolved, with perpetrators using social media to coerce, manipulate and threaten victims. The roles of those involved have blurred, as 'pimps' (the term used in Supreme Court cases to describe people who make money by controlling and selling others or sexual services) are now directly abusing children, making detection harder.[5]

Urban centres like Manila, Cebu City, and Angeles City remain hotspots for CSEC due to tourism, poverty and the global reach of digital platforms. While law enforcement efforts have improved, the rise of technology-facilitated exploitation has made these crimes more complex. Enhanced legal measures, digital monitoring and community awareness are crucial to protect vulnerable children.

[5] Childlight follows the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. This favours using the word 'facilitators' to describe people who make money from controlling or selling others for sexual services. However, the term 'pimps' is used here because it is used in legal contexts and widely referred to in the Philippines.

Shifting tactics and rising threats constitute the new face of child exploitation in the digital age.



## Methodology

This study used a secondary data analysis approach to review Philippine Supreme Court decisions on cases of online and offline CSEC from 2003 to 2024. The year 2003 was chosen as the starting point as it marks the enactment of the Anti-Trafficking in Persons Act (RA 9208), which is the first Philippine law to explicitly criminalise CSEC and establish a legal framework for prosecuting trafficking-related offenses. Using purposive sampling, only those legally adjudicated cases involving monetary or non-monetary exchange were included in order to ensure that the findings are based on definitive legal outcomes. Data were gathered from the Supreme Court e-library, using systematic search terms covering key Philippine laws on child sexual exploitation and abuse (CSEA). This resulted in 56 cases for final review and inclusion in the study.

A mixed method approach was employed combining quantitative analysis (descriptive statistics on offender profiles, modus operandi and case outcomes), with qualitative thematic analysis to identify patterns and trends in perpetration, enforcement and sentencing. Ethical approval was sought from the University of the Philippines Institutional Review Board and the University of Edinburgh to ensure privacy, data security and researcher well-being. By drawing from comprehensive legal records, this study provides a policy-relevant analysis of how technology has shaped CSEA in the Philippines, with the goal of strengthening child protection efforts in the Philippines.

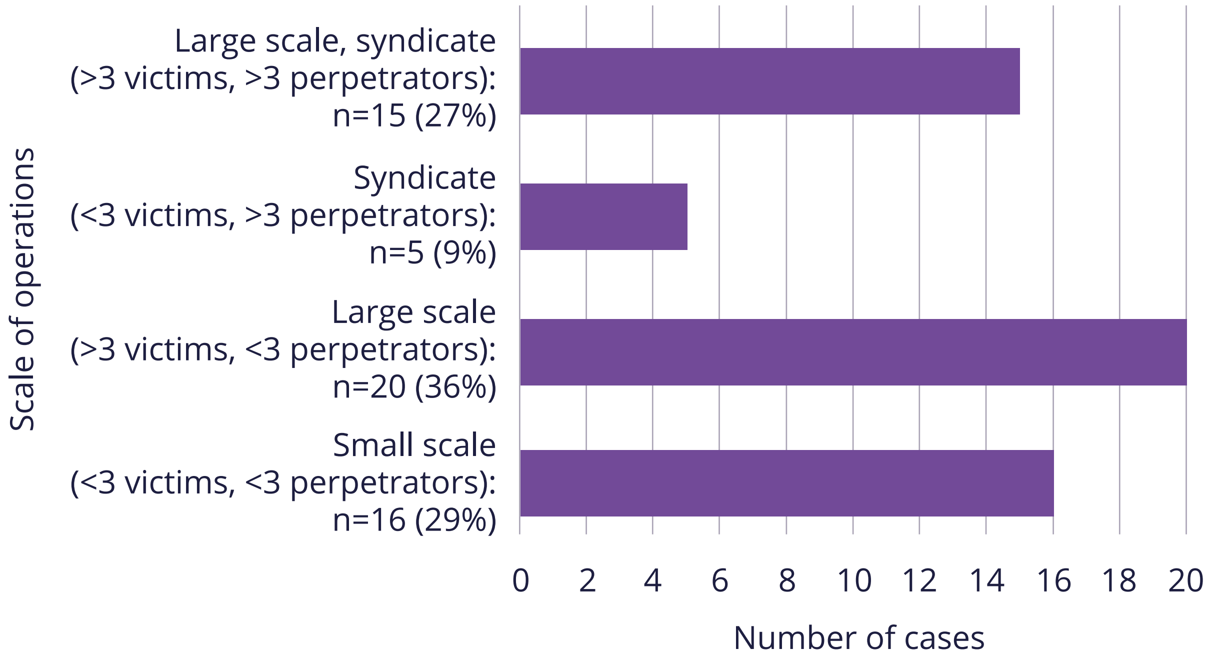
## Key findings

**Perpetrators:** In the CSEC cases studied, 51% of the perpetrators were women, who often acted as trusted family members or caregivers. Out of 160 identified perpetrators, ‘pimps’ (33%) were the main organisers, with some perpetrators also acting as recruiters (15%). Other offenders, such as hotel owners or karaoke television bar (KTV) operators (8%), provided venues for the exploitation. Some perpetrators were found to have directly abused victims (17%).

**Victim-perpetrator relationships:** Many perpetrators in the cases were known to their victims. Out of 85 identified relationships between victims and perpetrators, strangers introduced by third parties accounted for 46% of cases, while 17% of cases involved family members, 14% involved friends and 12% neighbours. Recent trends show a rise in younger victims (ages 5 to 12), often exploited by family members or acquaintances in online cases.

**Operations:** The majority of CSEC cases studied occurred in urban areas like Manila, Cebu, and Angeles City, where tourism and poverty drive demand for illicit services. Among the 56 reported cases, 36% involved large-scale operations where three or more children were victimised by one or two perpetrators. Another 27% also involved large-scale operations, but in these cases, the perpetrators were syndicates (i.e., three or more offenders). Meanwhile, 29% of cases involved small-scale operations, where one or two victims were exploited by one or two perpetrators. An additional 9% involved syndicates controlling one or two victims.

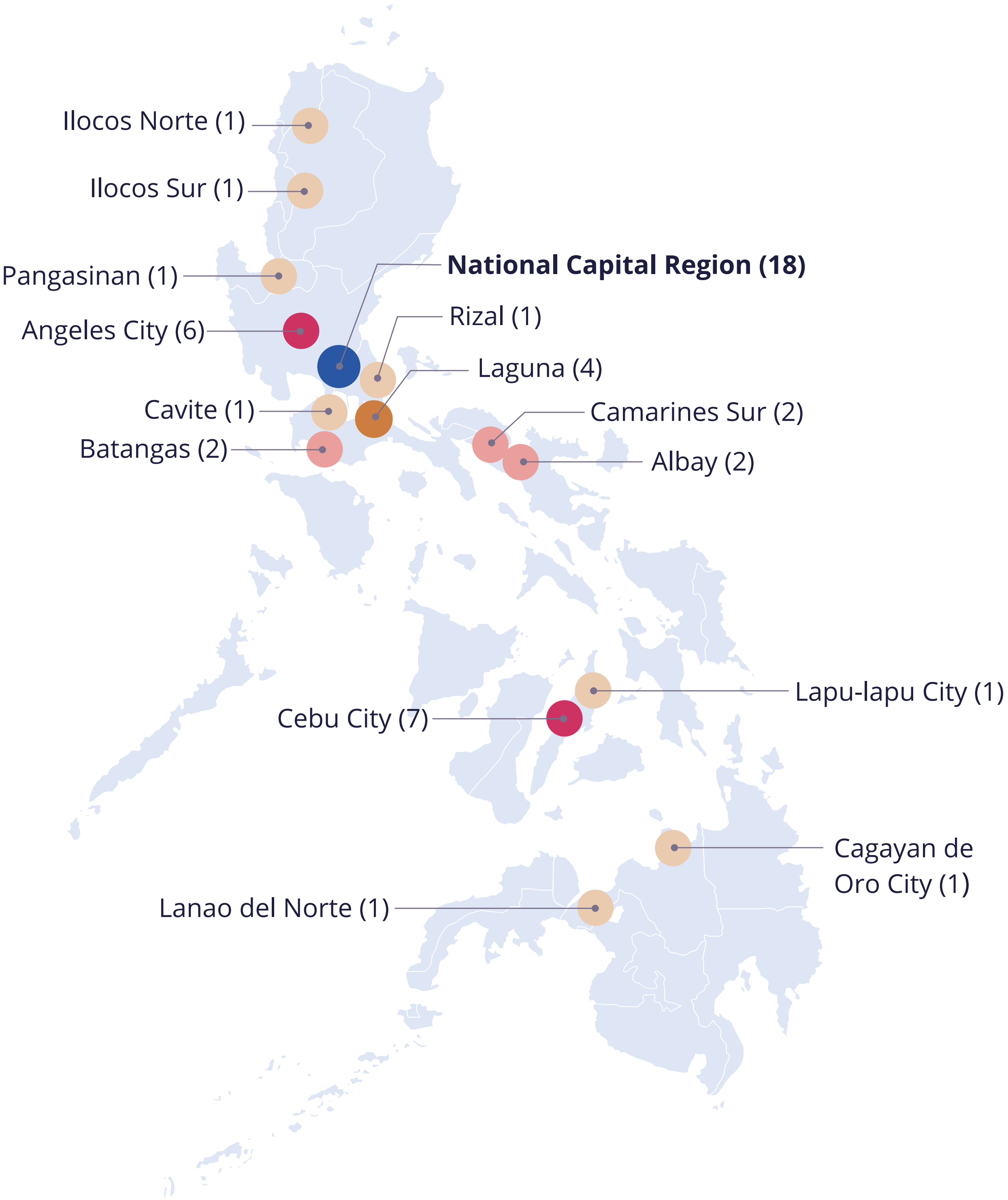
### Figure 1: Operations scale of commercial child sexual exploitation Supreme Court cases in the Philippines, 2003–2024, n=56



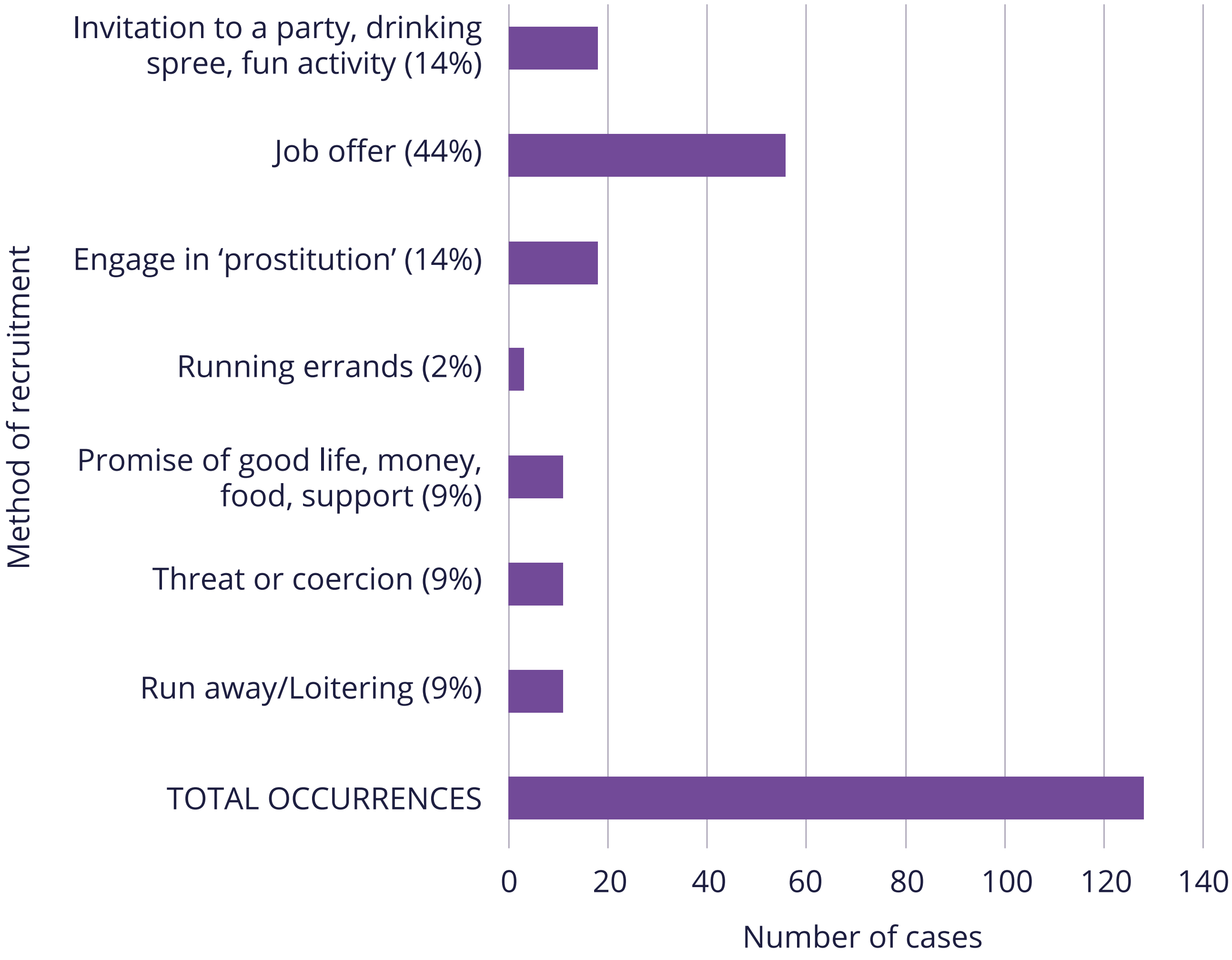
**Recruitment methods:** Common recruitment methods in the cases studied included false job offers (44%), invitations to social gatherings (14%), or direct invitations to engage in 'prostitution'[6] (14%). In online cases, coercion, threats, and manipulation (9%) were common tactics.

[6] Childlight follows the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. This favours use of the phrasing 'exploitation of children in/for prostitution' rather than 'child prostitution' to avoid stigmatising and harming children. However, the term 'prostitution' is used here because it is used in legal contexts and widely referred to in the Philippines.

## Figure 2: Geographic mapping of commercial child sexual exploitation Supreme Court cases in the Philippines, 2003–2024



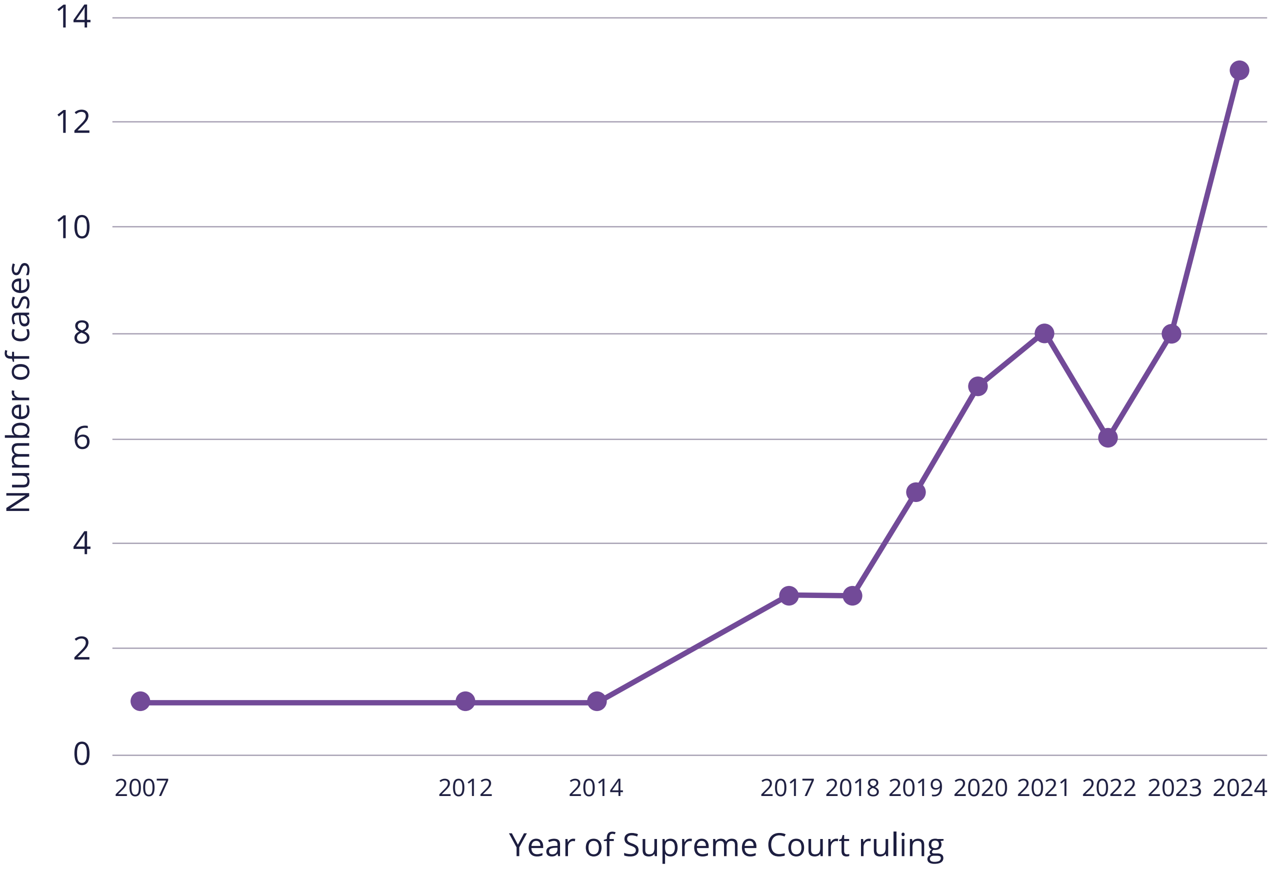
### Figure 3: Methods of recruitment identified in commercial child sexual exploitation Supreme Court cases in the Philippines, 2003–2024, n=128



**Financial transactions:** The financial transactions in CSEC cases varied. The lowest recorded amount was GBP 0.27 (27 British pence or around 20 Philippine pesos [PHP]), paid directly to a child for sexual contact. The average amount was GBP 134 (9,754 PHP), with the highest recorded payment at GBP 275 (20,017 PHP). Many transactions were facilitated through payment services or cryptocurrency.

**Law enforcement and case trends:** From 2007 to 2016, CSEC cases were relatively low, with only one to three cases per year. However, from 2017 onward, the number of cases steadily increased, reflecting improved detection and law enforcement efforts. In 2024, 13 cases were reported, 8 of which involved online exploitation. Technology-facilitated cases, like livestreaming abuse, have become more prominent in recent years, with the first livestreaming case brought to the Supreme Court in 2009.

### Figure 4: Supreme Court cases on commercial child sexual exploitation in the Philippines, 2007–2024



Note: Data points for 2008, 2009, 2010, 2011, 2013, 2015 and 2016 were not available.

**Disclosure, reporting, and arrests:** Many cases came to the attention of authorities through disclosure by children or tips from local and foreign sources. Law enforcement agencies like the Philippine National Police (PNP) and the National Bureau of Investigation (NBI) conduct surveillance and raids to rescue victims and arrest perpetrators. The effectiveness of the legal system relies on collaboration among government agencies, civil society organisations and the private sector. Global collaboration is critical, especially in technology-facilitated cases, where payment and internet service providers are criminally liable under the Philippine Republic Act (RA) 11930 (Anti-OSAEC Law) if they fail to prevent or report illicit transactions and activities linked to online child sexual exploitation.

In what is believed to be a first in the East Asia and Pacific region, this landmark legislation expands accountability beyond perpetrators and ensures that the companies enabling these crimes are also held responsible. Before RA 11930, there were already laws like RA 9775 (Anti-Child Pornography Act of 2009) and RA 10175 (Cybercrime Prevention Act of 2012) that required internet service providers (ISPs) to block and report abusive content, but these laws did not impose direct criminal liability on financial institutions. In an effort to strengthen child protection in the Philippines, RA 11930 recognises that not just abusers, but also the companies enabling these crimes, must be held responsible in keeping children safe online.

# Conclusion and recommendations

This study underscores the changing dynamics of CSEC in the Philippines, with a shift from large-scale operations to smaller, covert groups and an alarming rise in familial exploitation. The increasing use of digital platforms complicates detection and prosecution efforts. While legal frameworks and law enforcement have improved, significant gaps remain, particularly in addressing technology-facilitated crimes and holding all perpetrators accountable.

Key recommendations include:

**Recommendation 1.** Conduct community awareness programmes. Partner with non-profit organisations to educate the public on identifying and reporting CSEC, particularly in urban centres like Manila, Cebu, and Angeles City. A short, ten-minute video on human trafficking and CSEC should be distributed through schools, workshops, and social media to maximise reach.

**Recommendation 2.** Establish a case monitoring system. Collaborate with the Department of Justice's National Coordinating Council Against Online Sexual Abuse and Exploitation of Children (NCC-OSAEC) to create a digital platform to track CSEC cases in regional trial courts, ensuring transparency and accountability.

**Recommendation 3.** Put in place a unified hotline system. Consolidate child protection hotlines into a single, easy-to-remember number. Work with telecom companies to integrate these helplines into a digital platform and train volunteers to route calls to appropriate authorities.

**Recommendation 4.** Develop a unified referral system for the online sexual abuse and exploitation of children (OSAEC). Create a referral pathway that includes government agencies, non-profits, internet service providers (ISPs), and payment providers. This system should enable stakeholders to report suspicious content and transactions through a centralised platform linked to law enforcement.

**Recommendation 5.** Ensure support from local governments. Encourage local government units (LGUs) to adopt rules to enforce laws against OSAEC and child sexual abuse or exploitation material (CSAEM), including local monitoring teams and prevention campaigns.

**Recommendation 6.** Equip lawyers and law enforcement authorities with the skills to handle CSEC cases effectively. Provide targeted training for lawyers and law enforcement on handling CSEC cases, using real-life examples and interactive workshops to ensure effective case management.

**Recommendation 7.** Hold ISPs accountable for responding to child sexual abuse and exploitation content. Develop regulations for ISPs to respond quickly to reports of CSEC content, with a dedicated monitoring body to enforce compliance.

**Recommendation 8.** Provide victim support services. Increase access to trauma-focused counselling, legal aid, and financial support for victims through coordination with government and non-government organisations.

**Recommendation 9.** Implement poverty alleviation programmes. Introduce programmes to reduce the vulnerability of families in high-risk communities by providing sustainable livelihoods.

**Recommendation 10.** Enhance digital surveillance. Equip law enforcement with the tools to monitor online activities and collaborate with ISPs to identify offenders.

These recommendations aim to address both legal enforcement and public health strategies to protect children from exploitation and ensure their safety within their homes and communities.

## Limitations

This study is limited by the relatively small number of cases that reach the Supreme Court, especially given the Philippines' status as a hotspot for livestreamed sexual exploitation and abuse. Supreme Court cases tend to involve more serious, complex incidents, which may not reflect the full range of cases at lower court levels. Additionally, many cases involving plea bargaining do not proceed to the Supreme Court and cases dismissed at lower court levels were not accounted for.

## More information

**Suggested citation:** Martinez, A., Hernandez, S., Madrid., B., & Fry, D. (2025). Unmasking exploitation: Study of Supreme Court cases reveals changing landscape of CSEA in the Philippines. In: Searchlight 2025 – Who Benefits? Shining a Light on the Business of Child Sexual Exploitation and Abuse. Edinburgh: Childlight – Global Child Safety Institute

**Researchers:** Dr Andrea Martinez, Dr Sandra Hernandez, Dr Bernie Madrid and Professor Deborah Fry and students from De La Salle University Law School, Genary Kyna F. Gonzales, Kaori Kato, Airah Danelle M. Tuazon

**Study partners:** Child Protection Network, Department of Behavioral Sciences, University of the Philippines, Manila and National Institute of Health, University of the Philippines, Manila

**Registered study protocol:** OSF Registries | A Retrospective Study of the Profiles of Perpetrators of CSEC Cases

University of the Philippines, Manila, Research and Grants Administration Office (RGAO 2024-0766)

**Ethics approval:** University of the Philippines, Manila, Institutional Review Board (UPM REB 2024-0484-01) and University of Edinburgh, Childlight Research Ethics Sub-Committee (ARSPP-AMA-0240924CL).

**Advisory committee members:** Hon. Jose C. Reyes, Jr. (retired Associate Justice, Supreme Court of the Philippines and Chair of Philippine Judicial Academy Department of Special Areas of Concern), Dean Maria Concepcion S. Noche (Vice-Chair, Philippine Judicial Academy Department of Special Areas of Concern), Fiscal Lilian Doris S. Alejo (retired Senior State Prosecutor, Republic of the Philippines Department of Justice), Dean Sedfrey M. Candelaria (Chief, Philippine Judicial Academy Research, Publication and Linkages Office), Deputy Regional Prosecutor Barbara Mae Pagdilao-Flores (OIC – Executive Director Republic of the Philippines Department of Justice National Coordination Centre against Online Sexual Abuse and Exploitation and Child Sexual Abuse and Exploitation Material [NCC-OSAEC-CSAEM])

**Funding acknowledgement:** Funding acknowledgement: The research leading to these results has received funding from the Human Dignity Foundation under the core grant provided to Childlight – Global Child Safety Institute under the grant agreement number [INT21-01].

# Study H: Access denied: How blocklists are thwarting attempts to view CSAM

## Introduction

Domain blocking, or webpage blocking, has existed since the early 2000s as a virtual no-entry sign preventing people from accessing webpages known to contain child sexual abuse material (CSAM). It relies on ‘blocklists’ of specific website addresses (identified by organisations including the Internet Watch Foundation), which internet service providers (ISPs) cannot connect their users to when people search for them (Hunter, 2004). This study is the first to examine the extent to which people attempt to access blocked websites containing CSAM, coupled with the use of anonymisation services, which are tools people use to attempt to hide their identity and activities online. In doing so, we highlight the role these anonymisation services play in the ongoing dissemination and sharing of CSAM online. This can help guide regulators and ISPs in better preventing access to CSAM by improving detection methods to stop attempts to bypass website blocking.

## Methodology

To gauge the blocking of attempts to access webpages known to contain CSAM using devices such as mobile phones and laptops, Childlight examined data from a global partner that operates the Domain Name Service (DNS). The DNS acts like both an address book for the internet and an operator, allowing users who search for a website through their ISP to be connected to where they wish to be. Blocked webpages are cross-referenced with regularly updated lists held by the Internet Watch Foundation as well as law enforcement agencies, including INTERPOL. In addition to looking at the number of search requests that are blocked (blocked requests), further data was analysed around additional requests by the same requesting users for a 48-hour period. This resulted in a dataset prepared for a consecutive two-day period in September 2024, which Childlight analysed.

## Glossary of terms

**Internet Protocols (IP addresses):** Unique identifying numbers assigned to all devices that connect to the internet, including phones, laptops, tablets, modems and servers.

**Domain Name Service (DNS):** A company that receives requests from users through internet service providers and connects the users with the requested webpages.

**Virtual Private Network (VPN):** A service that allows users to send their request through an alternate route.

**The Onion Router (TOR):** The most common browser used to connect to the Dark Web where CSAM is displayed on encrypted hidden pages.

**Proxies:** A middle device used to connect a user with the website they are requesting.

**Internet Service Providers (ISPs):** Companies that connect users to the internet.

**Electronic Service Providers:** Companies that offer online services like messaging, payments or cloud storage.

**Web crawlers:** Technological tools developed to visit large volumes of webpages simultaneously, without consideration of what is on the page, to scan and detect content for various purposes. As such, web crawlers often visit the same webpages daily or at times more frequently to gather as much data as possible.

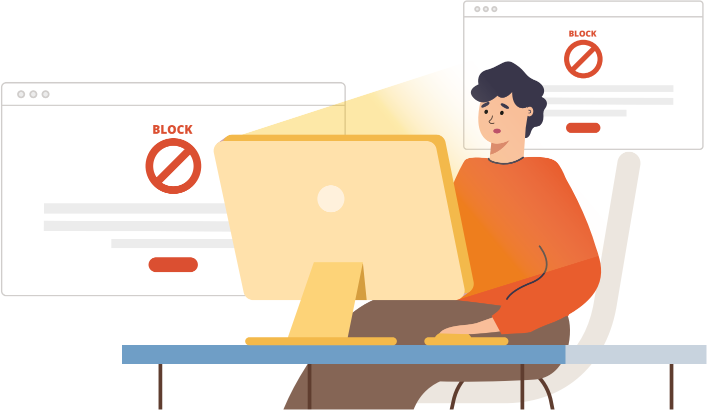
The dataset included all confirmed and suspected CSAM page requests, globally organised by indicators. These indicators included the geographic area where the request was first received, the number of requesting users seeking known CSAM webpages and the use of anonymisation services. Anonymisation services are web-based tools that users can employ in order to mask, mislead or misrepresent who they are and their location. These include proxies, where internet traffic first goes through another computer as an intermediary before reaching the website the requesting user wants to visit. They also include virtual private networks (VPNs), in which online activity is encrypted and routed through a server in another location. A third tool is The Onion Router (TOR), a browser and network that bounces a user's internet connection through several different computers around the world and can be used to access the Dark Web.

## Key findings

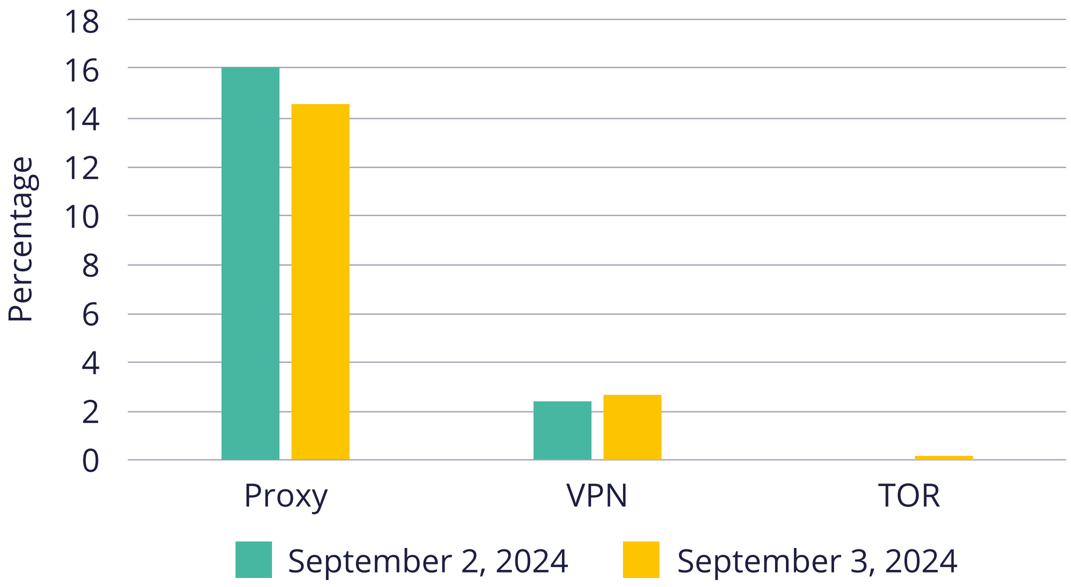
Over two days, more than 853,000 attempts to access webpages with CSAM were successfully blocked. This means there were about five attempts every second worldwide to reach illegal content or around 156 million attempts per year.

Many of the people trying to access CSAM used anonymisation services like proxies and VPNs to hide their identity. However, most of the requests studied did not use these such services. Only 15% of CSAM requests used proxies and 2.5% used VPNs, indicating that most of the users were not trying to hide their activities with anonymisation tools. Proxies and VPNs were used more often for other types of content, not specifically CSAM.

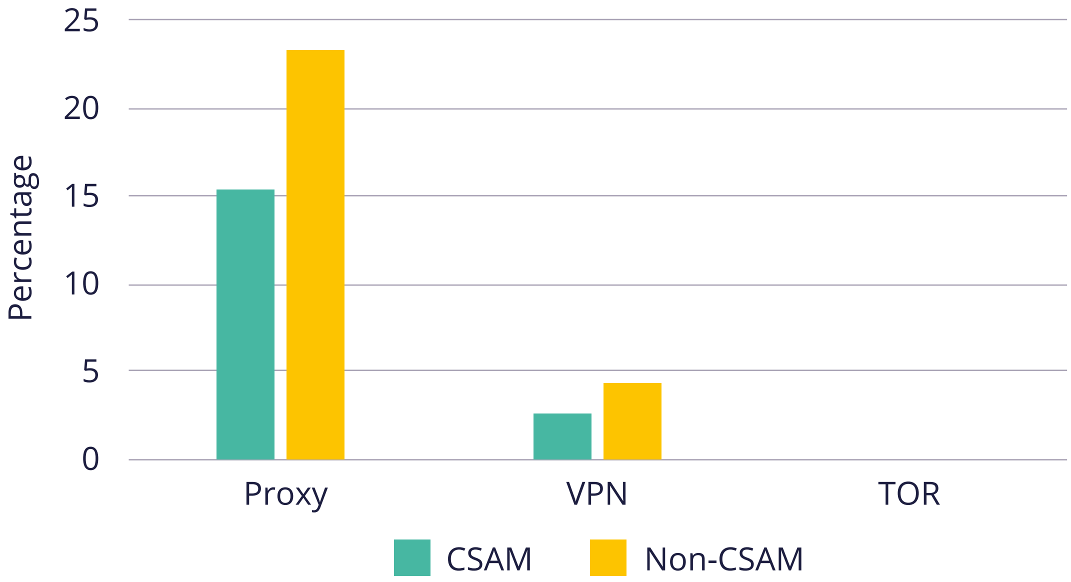
Internet users attempt to access banned content five times every second.



### Figure 1: Anonymisation use for CSAM domains by date



### Figure 2: Anonymisation use for CSAM and non-CSAM requests



When it comes to TOR, a browser used to access the Dark Web, it made up less than 1% of all CSAM-related requests. This is different from accessing hidden websites on the Dark Web itself, where CSAM is more commonly found. However, in some countries, TOR was used more frequently for CSAM searches. For example, Germany had the most TOR requests for CSAM according to the blocked webpage data, although these only made up 1% of Germany's total TOR activity as identified in this data. Moldova had a high percentage of TOR requests for CSAM, though the total number was very small.

In total, 12 countries had webpage activity linked only to CSAM. The highest number of device requests from a specific country came from Singapore, with 223 cases of devices making CSAM-only requests over two days. This highlights the global nature of the issue.

# Recommendations

**Recommendation 1.** All internet service providers should be required to block websites known to contain CSAM. Due to the way the internet operates, often a single webpage request will be carried out in part by multiple service providers. The more ISPs that utilise this service, the greater the likelihood that any individual query will be flagged to be blocked by one of the services.

**Recommendation 2.** Ensure that blocklists are shared more widely with internet service providers, electronic service providers and social media companies so they are able to block the sharing of links within their respective platforms. This will also help platforms better identify, and respond to, bad actors who are attempting to share access to CSAM through their services.

**Recommendation 3.** Put in place regulation and oversight of the points where users connect to, and exit from, the TOR network. This was the only anonymisation service that was used more often for known CSAM domain requests than other requests made by the same requesting users. By regulating the number of users able to access TOR, it will not only limit the number of users attempting to access blocked CSAM webpages, but also the known CSAM that exists on '.onion' domains that can only be accessed through TOR.

**Recommendation 4.** Governments should monitor blocked access to CSAM domains to help identify areas for improvement in terms of security risks and online safety.

**Recommendation 5.** When blocked domain requests are relayed, provide an option for support services to those requesting the domain, such as StopItNow.org.uk.

# Limitations

The data referred to in this study is limited by the short period it covers and because it only looked at users who had attempted to access at least one known CSAM webpage. The overall numbers may be inflated due to the possible inclusion of web crawlers, which seek access to numerous webpages every day without consideration of the content displayed on each requested domain. The data may also include multiple requests from the same user(s) within the period. Finally, it is important to note that this analysis does not consider attempts to view webpages containing CSAM which are not on active blocked lists.

## More information

**Suggested citation:** Stevenson, J., Mclean, L., & Fry, D. (2025). Access denied: How blocklists are thwarting attempts to view CSAM. In: Searchlight 2025 – Who Benefits? Shining a Light on the Business of Child Sexual Exploitation and Abuse. Edinburgh: Childlight – Global Child Safety Institute

**Researchers:** Mr James Stevenson, Mr Lewis McLean, Professor Deborah Fry

**Study partners:** Cisco Umbrella DNS

**Registered study protocol:** OSF | Web Anonymisation Service Access for Child Sexual Abuse Material

**Ethics approval:** University of Edinburgh, Childlight Research Ethics Sub-Committee (CATTU-JST-0060424CL)

**Advisory committee members:** Hugh Dixon (Nominet), Joanne Negrette (Cisco), Lloyd Richardson (Canadian Centre for Child Protection)

**Funding acknowledgement:** The research leading to these results has received funding from the Human Dignity Foundation under the core grant provided to Childlight – Global Child Safety Institute under the grant agreement number [INT21-01].

# Searchlight 2025 Conclusion

Searchlight 2025 shines new light on the nature of child sexual exploitation and abuse, offering important evidence and insights into the complex web of beneficiaries profiting from what has become a multi-billion-dollar industry. This is a deliberately diverse set of studies, but what they have in common is that each represents a disturbing dimension of a global pandemic — and each requires action now.

We have seen how organised criminals and individuals profit by exploiting gaps in law and technology, sometimes operating in the darkest recesses of the internet, sometimes in plain sight. We have highlighted how abusers target at-risk groups, whether on dating apps or in war zones. And, we have pointed out the potentially growing commercialised nature of familial abuse in the Philippines, with the worth of a child reduced to as little as 27 British pence or 34 US cents — the cost for one perpetrator to commit sexual abuse against a child.

Of course, the greatest cost is the impact to millions of children whose lives are forever altered by the consequences that CSEA can exact on their health and prospects, limiting their life chances. We know this to be true, not just from multiple studies that have revealed the links to negative mental and physical health, negative education outcomes and reduced employment, but also from many inquiries into non-recent child sexual abuse, in which survivors have shared their accounts.

It is clear that more support mechanisms for survivors are required, including therapeutic programmes for recovery and to help them navigate the complexities of criminal justice systems, as well as global restitution as an essential step in their healing and rehabilitation.

Crucially, those in positions of power to influence how the world responds to CSEA must also realise that this problem is preventable, not inevitable. As with other pandemics, such as Covid-19 and HIV/AIDS, the world needs to come together to provide a comprehensive public health response.

We must be alive to, and anticipate, emerging threats like AI-generated CSAM, and have the legislation and regulations in place to protect children — using AI and other technologies not just to keep pace with, but to get ahead of, the issue. As we have shown, preventive steps like webpage blocking can be highly effective and give real grounds for optimism.

Implementing the recommendations in this report — with energy and commitment from governments, tech companies and everyone involved in protecting children — can also make a real difference in tackling this public health emergency to help ensure we do not fail a generation. And the time to act is now, because children can’t wait.

# Acknowledgements

These studies would not have been possible without the support of Human Dignity Foundation, which established Childlight as an independent data institute hosted by the University of Edinburgh and the University of New South Wales. The research team would also like to thank Jesuit Social Services for funding two of the studies. Special thanks are due to our key Childlight research hub partnerships including Universidad de los Andes, University of New South Wales and University of the Philippines, Manila.

Special thanks also go to the International Society for the Prevention of Child Abuse and Neglect (ISPCAN) where these studies were presented in Autumn of 2024 to a global forum of key practitioners and academics. We would like to thank all our advisory committee members for this Searchlight Report, our Childlight Ethics Review Committee, and the Childlight Steering Board for their ongoing support to Childlight in our goal of producing rigorous and robust data and to report that data without fear or favour.

# References

## Study A: Clicks for cash

Acar, K.V. (2017). Child abuse materials as digital goods: Why we should fear new commercial forms. Economics Discussion Papers, No. 2017-15. Kiel: Kiel Institute for the World Economy (IfW).

Anglia Ruskin University (ARU), and Internet Watch Foundation (IWF). (2024). “It’s normal these days.” Self-generated child sexual abuse fieldwork findings report. ARU International Policing and Public Protection Research Institute and IWF. https://www.iwf.org.uk/media/i40cdajw/final-self-generated-child-sexual-abuse-fieldwork-findings-report-by-pier_may_2024.pdf

Canadian Centre for Child Protection (C3P). (2022). An analysis of financial sextortion victim posts published on r/sextortion. C3P. https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

Canadian Centre for Child Protection (C3P). Online harms: Sextortion. Cybertip.ca. (2024). https://cybertip.ca/en/online-harms/sextortion/

Friel, S., Collin, J., Daube, M., Depoux, A., Freudenberg, N., Gilmore, A.B., Johns, P., Laar, A., Marten, R., McKee, M., & Mialon, M. (2023). Commercial determinants of health: future directions. Lancet, 8 April 2023, 401(10383): 1229–1240.

Fry, D., Krzeczkowska, A., Anderson, N., Ren, J., McFeeters, A., Lu, M., Vermeulen, I., Jaramillo, K., Marmolejo Lozano, M.P., Savadova, S., Kurdi, Z., Jin, W., Zhang, J., Liu, W., Lu, Y., Shangguan, S., Zhu, Y., Zhu, H., Gong, X., Lio, J., Harker-Roa, & Fang, X. (2024). Indicator 1: The prevalence of online victimisation [Online]. Data from ‘Into the Light: Childlight’s Global Child Sexual Exploitation and Abuse Index’. Edinburgh: Childlight. https://intothelight.childlight.org/indicator-1.html

Fry, D., Krzeczkowska, A., Ren, J., Lu, M., Fang, X., Anderson, N., Jin, W., Liu, W., Vermeulen, I., McFeeters, A., Harker-Roa, A., Jaramillo Diaz, K., Kurdi, Z., Marmolejo Lozano, M. P., Olié, L., Savadova, S., Shangguan, S., Zhang, J., Zhu, H., …Steele, B. (2025). Prevalence estimates and nature of online child sexual exploitation and abuse: a systematic review and meta-analysis. The Lancet Child and Adolescent Health, 9(3), 184–193. https://doi.org/10.1016/S2352-4642(24)00329-8

Internet Watch Foundation (IWF). (2023). Sexually coerced extortion or “sextortion”: IWF 2023 Annual Report. IWF. https://www.iwf.org.uk/annual-report-2023/trends-and-data/sexually-coerced-extortion/

Malby, S., Jesrani, T., Banuelos, T., Holterhof, A., & Hahn, M. (2015). Study on the effects of new information technologies on the abuse and exploitation of children. United Nations Office on Drugs and Crime (UNODC). https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf

Meggyesfalvi, B. (2024). Challenges in investigating self-generated online child sexual abuse material. Belügyi Szemle, 72(2), 329–339. https://doi.org/10.38146/BSZ.2024.2.8

National Center for Missing and Exploited Children (NCMEC). (2017). The online enticement of children: An in-depth analysis of Cybertipline reports. NCMEC. https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Online%20Enticement%20Pre-Travel1.pdf

Prakash, G.A., Sundaram, A., & Sreeya, B. (2021). Online exploitation of children and the role of intermediaries: an Indian legislative and policy perspective. International Review of Law, Computers and Technology, 36(3), 431–452. https://doi.org/10.1080/13600869.2021.1999290

Ramiro, L.S., Martinez, A.B., Tan, J.R.D., Mariano, K., Miranda, G.M.J., & Bautista, G. (2019). Online child sexual exploitation and abuse: A community diagnosis using the social norms theory. Child Abuse and Neglect, 96, 104080.

Reeves, L. (2023). Internet matters x Nominet research: Young people’s views on preventing nude image-sharing [online]. Internet Matters, 11 December 2023. https://www.internetmatters.org/hub/research/nominet-research-young-people-views-preventing-nude-image-sharing/

Roos, H. (2014). Trading the sexual child: Child pornography and the commodification of children in society. Texas Journal of Women and the Law, 23(2), 131–156. https://www.proquest.com/scholarly-journals/trading-sexual-child-pornography-commodification/docview/1552700633/se-2

Salter, M., & Sokolov, S. (2024). “Talk to strangers!” Omegle and the political economy of technology-facilitated child sexual exploitation. Journal of Criminology (2021), 57(1), 121–137. https://doi.org/10.1177/26338076231194451

Schulz, P. (2018). Children as commodities: Conflicting discourses of protection and abuse of children. Children Australia, 43(4), 231–244. https://doi.org/10.1017/cha.2018.43

Statista. (July 22, 2024). Social media advertising spending worldwide from 2019 to 2029 (in billion U.S. dollars) [graph, online]. Statista, 22 July 2024. https://www-statista-com.eux.idm.oclc.org/forecasts/1418549/social-media-ad-spend-worldwide (accessed 17 February 2025).

Vaughan, E. H. (2024). NCMEC releases new sextortion data. Blog, National Center for Missing and Exploited Children (NCMEC), 15 April 2024. https://www.missingkids.org/blog/2024/ncmec-releases-new-sextortion-data

World Advertising Research Centre. (2024, May). Social media trends: 2024 global report [online]. World Advertising Centre. https://www.gwi.com/reports/social

## Additional reading

Carpinteri, A., Bang, B., Klimley, K., Black, R.A., & Van Hasselt, B. (2018). Commercial sexual exploitation of children: An assessment of offender characteristics. Journal of Police and Criminal Psychology, 33(2), 150–157. https://doi.org/10.1007/s11896-017-9242-0

Cybertip.ca. (2024). Online harms: Sextortion [online]. Cybertip.ca. https://cybertip.ca/en/online-harms/sextortion/

Europol. (2020). Exploiting isolation: Offenders and victims of online child sexual abuse during the Covid-19 pandemic. Europol. https://www.europol.europa.eu/sites/default/files/documents/europol_covid_report-cse_jun2020v.3_0.pdf

Giles, S., & Alison, L. (2021). Prioritizing indecent image offenders: A systematic review and economic approach to understand the benefits of evidence-based policing strategies. Frontiers in Psychology, 12, 606731. https://doi.org/10.3389/fpsyg.2021.606731

Giles, S., Alison, L., Humann, M., Tejeiro, R., & Rhodes, H. (2024). Estimating the economic burden attributable to online only child sexual abuse offenders: Implications for police strategy. Frontiers in Psychology, 14, 1285132. https://doi.org/10.3389/fpsyg.2023.1285132

Laurie, S.R., Martinez, A.B., Tan, J.R.D., Mariano, K., Miranda, G.M.J., & Bautista, G. (2019). Online child sexual exploitation and abuse: A community diagnosis using the social norms theory. Child Abuse and Neglect, 96, 104080. https://doi.org/10.1016/j.chiabu.2019.104080

Mujica, J. (2013). The microeconomics of sexual exploitation of girls and young women in the Peruvian Amazon. Culture, Health and Sexuality, 15, 2013, S141–S152. http://www.jstor.org.eux.idm.oclc.org/stable/23524457

Steel, C.M.S., Newman, E., O’Rourke, S., & Quayle, E. (2023). Lawless space theory for online child sexual exploitation material offending. Aggression and Violent Behavior, 68, 101809. https://doi.org/10.1016/j.avb.2022.101809

Tsaliki, L. (2016). Children and the politics of sexuality: The sexualization of children debate revisited. Palgrave Macmillan. https://doi.org/10.1057/978-1-137-03341-3

## Study B: Where does the money flow?

Alianza Global WeProtect. (2021). Evaluación de la amenaza global de 2021: Trabajamos juntos para poner fin al abuso sexual infantil a través de internet. Alianza Global WeProtect. https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2021-Report_Spanish.pdf

Aronowitz, A.A., & Veldhuizen, M. E. (2021). The human trafficking-organized crime nexus. In: Felia Allum and Stan Gilmour, Routledge Handbook of Transnational Organized Crime. London: Routledge, pp 232–252.

Brown, R., Napier, S., & Smith, R.G. (2022). Australians who view live streaming of child sexual abuse: An analysis of financial transactions. Trends and Issues in Crime and Criminal Justice No. 589. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04336

Celiksoy, Ergul, Schwarz, Katarina, Sawyer, Laura, & Ciucci, Sara. (2023). Payment methods and investigation of financial transactions in online sexual exploitation of children cases. University of Nottingham Rights Lab and Global Fund to End Modern Slavery. https://www.nottingham.ac.uk/research/beacons-of-excellence/rights-lab/resources/reports-and-briefings/2023/october/payment-methods-and-investigation-of-financial-transactions-in-online-sexual-exploitation-of-children-cases.pdf

Childlight. (2024). The Light Index executive summary [online]. Childlight– Global Child Safety Institute. https://intothelight.childlight.org/executive-summary.html

Demarest, H.M. (2015). The scarlet market: The economic framework of sex trafficking and microfinance as a proactive solution. Honours Thesis, Southeastern University, Lakeland. https://firescholars.seu.edu/cgi/viewcontent.cgi?article=1002&context=honors

ECPAT. (2016). Offenders on the move: Global study on sexual exploitation of children in travel and tourism. Bangkok: Every Child Protected against Trafficking (ECPAT) International. https://ecpat.org/wp-content/uploads/2021/08/Global-Report-Offenders-on-the-Move.pdf

Hopkins, M., Keighley, R., & Sanders, T. (2024). Organised crime and the ecosystems of sexual exploitation in the United Kingdom: How supply and demand generate sexual exploitation and protection from prosecution. Trends in Organized Crime, 27(1), 56–76.

Kara, S. (2017). Sex trafficking: Inside the business of modern slavery. New York: Columbia University Press.

Krylova, Y., & Shelley, L. (2023). Criminal street gangs and domestic sex trafficking in the United States: evidence from Northern Virginia. Crime, Law and Social Change, 80(3), 307–328.

Lasonder, J., & Fiander, A. (2024). Sexual exploitation. In: A. Fiander and J. Lasonder, Health and Slavery: A Healthcare Provider's Guide to Modern Day Slavery and Human Trafficking. Cham: Springer, pp. 57–63.

Lugo, K. (2020). Gang sex trafficking in the United States. In: J. Winterdyk and J. Jones (eds), The Palgrave International Handbook of Human Trafficking, pp. 521–540.

Meyer, O. (2018). City of Roses: Sexual exploitation in Portland, Oregon. Thesis, Concordia University, Portland. https://digitalcommons.csp.edu/cup_commons_undergrad/18/

Miller-Perrin, C., & Wurtele, S.K. (2017). Sex trafficking and the commercial sexual exploitation of children. Women and Therapy, 40(1–2), 123–151.

Palacios, S.P.I. (2022). Las lucrativas redes de tráfico de mujeres de México y Centroamérica para el comercio sexual en Estados Unidos. Latin American Research Review, 57(3), 608–626.

Rai, R., & Rai, A.K. (2021). Nature of sex trafficking in India: A geographical perspective. Children and Youth Services Review, 120, 105739.

Roche, S., Otarra, C., Fell, I., Torres, C.B., & Rees, S. (2023). Online sexual exploitation of children in the Philippines: A scoping review. Children and Youth Services Review, 148, 106861.

Van der Bruggen, M., & Blokland, A. (2021). Child sexual exploitation communities on the Darkweb: How organized are they?. In: M.W. Kranenbarg and R. Leukfeldt, Cybercrime in Context: The Human Factor in Victimization, Offending, and Policing. Cham: Springer International Publishing, pp. 259–280.

WeProtect Global Alliance. (2021). Global threat assessment 2021. WeProtect Global Alliance. https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2021.pdf

Williams, J., Lim, C., Trull, V., & Higgins, M. (2021). The commercial sexual exploitation of children. In: R. Geffner, J.W. White, L.K. Hamberger, A. Rosenbaum, V. Vaughan-Eden, and V.I. Vieth, Handbook of Interpersonal Violence and Abuse Across the Lifespan: A Project of the National Partnership to End Interpersonal Violence Across the Lifespan (NPEIV). Cham: Springer International Publishing, pp. 907–930.

Wurtele, S.K. (2017). Understanding and preventing the sexual exploitation of youth. In: J Stein, Reference Module in Neuroscience and Biobehavioral Psychology. Elsevier.

## Additional reading

Aronowitz, A.A. (2012). The human trafficking–organized crime nexus. In: Felia Allum and Stan Gilmour, Routledge Handbook of Transnational Organized Crime. London: Routledge, pp. 217–233.

Chainalysis. (2024). The 2024 crypto crime report. Chainalysis. https://www.chainalysis.com/wp-content/uploads/2024/06/the-2024-crypto-crime-report-release.pdf

Currie, G. (2024). Dating app beast targeted single Scots mothers to gain access to their children. Daily Record, 9 December 2024. https://www.dailyrecord.co.uk/news/scottish-news/scots-paedophile-lorry-driver-sexually-34279018

Martínez Herrera, L.A. (2017). Contrabando, narcomenudeo y explotación sexual en Pereira, Colombia. Revista Mexicana de Sociología, 79(3), 459-486.

Teunissen, C., Thomsen, D., Napier, S., & Boxall, H. (2024). Risk factors for receiving requests to facilitate child sexual exploitation and abuse on dating apps and websites. Trends and Issues in Crime and Criminal Justice No 686. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti77291

Tripp, T. M., & McMahon-Howard, J. (2016). Perception vs. reality: The relationship between organized crime and human trafficking in metropolitan Atlanta. American Journal of Criminal Justice, 41, 732–764.

## Study C: Following the money

Chainalysis. (2024). The 2024 crypto crime report. Chainalysis. https://www.chainalysis.com/wp-content/uploads/2024/06/the-2024-crypto-crime-report-release.pdf

## Study D: Swipe wrong

Currie, G. (2024). Dating app beast targeted single Scots mothers to gain access to their children. Daily Record, 9 December 2024. https://www.dailyrecord.co.uk/news/scottish-news/scots-paedophile-lorry-driver-sexually-34279018

Teunissen, C., Thomsen, D., Napier, S., & Boxall, H. (2024). Risk factors for receiving requests to facilitate child sexual exploitation and abuse on dating apps and websites. Trends and Issues in Crime and Criminal Justice No 686. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti77291

## Study E: Hidden casualties of war

Child Helpline International, 2024, Country Report HUNGARY MHPSS Services for Refugees from Ukraine. https://childhelplineinternational.org/wp-content/uploads/2024/08/Country-Report-Hungary.pdf

ECPAT. (2020). Summary paper on online child sexual exploitation. Bangkok: Every Child Protected against Trafficking (ECPAT). https://ecpat.org/wp-content/uploads/2021/05/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf (accessed 1 February 2024).

Guterres, A. (2022). Secretary-General’s opening remarks to the press on the war in Ukraine [online]. United Nations, 14 March 2022. https://www.un.org/sg/en/content/sg/speeches/2022-03-14/opening-remarks-the-press-the-war-ukraine%C2%A0 (accessed 23 February 2024).

Guardian, The. (2023). Ukrainian refugees increasingly targeted for sexual exploitation, research finds. The Guardian, 26 March 2023. https://www.theguardian.com/world/2023/mar/26/ukrainian-refugees-increasingly-targeted-for-sexual-exploitation-research-finds (accessed 23 February 2024).

Marsh, M., Purdin, S., & Navani, S. (2006). Addressing sexual violence in humanitarian emergencies. Global Public Health, 1(2), 133–146. https://doi.org/10.1080/17441690600652787

OCHA. (2024). Global humanitarian overview 2024 [online]. OCHA, 11 December 2023. https://www.unocha.org/publications/report/world/global-humanitarian-overview-2024-enarfres (accessed 1 February 2024).

Spangaro, J., Adogu, C., Ranmuthugala, G., Powell Davies, G., Steinacker, L., & Zwi, A. (2013). What evidence exists for initiatives to reduce risk and incidence of sexual violence in armed conflict and other humanitarian crises? A systematic review. PLoS ONE, 8(5). https://doi.org/10.1371/journal.pone.0062600

UNICEF. (2024a). Children under attack [online]. United Nations Children's Fund. https://www.unicef.org/children-under-attack (accessed 1 February 2024).

UNICEF. (2024b). Sexual violence against children [online]. United Nations Children's Fund. https://www.unicef.org/protection/sexual-violence-against-children (accessed 1 February 2024).

UNICEF. (2024c). Six grave violations against children in times of war [online]. United Nations Children's Fund. https://www.unicef.org/stories/children-under-attack-six-grave-violations-against-children-times-war#:~:text=Six%20grave%20violations%20against%20children%20in%20times%20of,6.%20Denial%20of%20humanitarian%20access%20for%20children%20 (accessed 1 February 2024).

## Additional reading

ECPAT. (2018). Towards a global indicator on unidentified victims in child sexual exploitation material: Summary report [online]. Bangkok: Every Child Protected against Trafficking (ECPAT). https://www.ecpat.org.uk/towards-a-global-indicator-on-child-sexual-exploitation-material (accessed 1 February 2024).

Internet Watch Foundation (IWF). (2020). Millions of attempts to access child sexual abuse online during lockdown [online]. IWF News. https://www.iwf.org.uk/news-media/news/millions-of-attempts-to-access-child-sexual-abuse-online-during-lockdown/ (accessed 23 February 2024).

INTERPOL. (2023). Our analysis reports [online]. INTERPOL. https://www.interpol.int/en/How-we-work/Criminal-intelligence-analysis/Our-analysis-reports (accessed 1 February 2024).

NCMEC. (2021). CyberTipline 2021 report. National Center for Missing and Exploited Children (NCMEC). https://www.missingkids.org/content/dam/missingkids/pdfs/2021-CyberTipline-Report.pdf (accessed 1 February 2024).

NCMEC. (2023). CyberTipline 2023 report. National Center for Missing and Exploited Children (NCMEC). https://www.missingkids.org/content/dam/missingkids/pdfs/2023-CyberTipline-Report.pdf (accessed 1 February 2024).

NSPCC. (2020). Isolated and struggling. Social isolation and the risk of child maltreatment, in lockdown and beyond. National Society for the Prevention of Cruelty to Children (NSPCC). https://learning.nspcc.org.uk/media/2246/isolated-and-struggling-social-isolation-risk-child-maltreatment-lockdown-and-beyond.pdf (accessed 23 February 2024).

NSPCC. (2022). Online grooming crimes have risen by more than 80% in four years [online]. National Society for the Prevention of Cruelty to Children (NSPCC). https://www.nspcc.org.uk/about-us/news-opinion/2022/online-grooming-crimes-rise/ (accessed 1 February 2024).

One in Four. (2024). About one in four [online]. One in Four. https://oneinfour.org.uk/about-one-in-four/ (accessed 1 February 2024).

WHO. (2022). What works to prevent online violence against children? Executive Summary. Geneva: World Health Organization. https://www.who.int/publications/i/item/9789240062085

## Study F: Legal challenges in tackling AI-generated CSAM

The references for this report are particularly extensive and can be viewed in the technical note.

Australian Government, Department of Industry, Science & Resources. (2024). Safe and Responsible AI in Australia: Proposals Paper for Introducing Mandatory Guardrails for AI in High-Risk Settings. Australian Government. https://consult.industry.gov.au/ai-mandatory-guardrails

Gawne, E. (2024). Man who made 'depraved' child images with AI jailed. BBC News, 28 October 2024. BBC News, Manchester. https://www.bbc.com/news/articles/cq6l241z5mjo (accessed 10 February 2025).

Home Office. (2025). Britain's leading the way protecting children from online predators. UK Government, Home Office. https://www.gov.uk/government/news/britains-leading-the-way-protecting-children-from-online-predators#:~:text=make%20it%20illegal%20to%20possess,to%203%20years%20in%20prison

Lexology. (2025). Prorogation's Digital Impact: Canada's Digital Bills Set to Die on the Order Paper. Lexology. https://www.lexology.com/library/detail.aspx?g=5e9b0d85-d01d-42e9-8a51-f1ad1bce0956&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=Australian+IHL+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2025-01-21&utm_term

Minister for Communications. (2025). Report of the Online Safety Act Review released. Minister for Communications. https://minister.infrastructure.gov.au/rowland/media-release/report-online-safety-act-review-released

OFCOM. (2024). Protecting people from illegal harms online Illegal Content Judgements Guidance (ICJG). OFCOM. https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/illegal-content-judgements-guidance-icjg.pdf?v=387556

OFCOM. (2025). Guide for services: complying with the Online Safety Act. OFCOM. https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/guide-for-services/

## Study G: Unmasking exploitation

## Additional reading

Ali, S., Haykal, H. A., & Youssef, E. Y. M. (2023). Child sexual abuse and the internet — A systematic review. Human Arenas, 6(2), 404–421.

Blancaflor, E., Balita, L. B. S., Subaan, V. R. S., Torres, J. A. D. F., & Vasquez, K. J. P. (2022, December). Implications on the prevalence of online sexual exploitation of children (OSEC) in the Philippines: A cybersecurity literature review. In: 2022 5th International Conference on Computing and Big Data (ICCBD). IEEE, pp. 34–38.

Cale, J., Holt, T., Leclerc, B., Singh, S., & Drew, J. (2021). Crime commission processes in child sexual abuse material production and distribution: A systematic review. Trends and Issues in Crime and Criminal Justice, (617), 1–22.

Carpinteri, A., Bang, B., Klimley, K., Black, R. A., & Van Hasselt, V. B. (2018). Commercial sexual exploitation of children: An assessment of offender characteristics. Journal of Police and Criminal Psychology, 33, 150–157.

Chiu, J., & Quayle, E. (2022). Understanding online grooming: An interpretative phenomenological analysis of adolescents' offline meetings with adult perpetrators. Child Abuse and Neglect, 128, 105600.

Christensen, L.S., & Tsagaris, G. S. (2020). Offenders convicted of child sexual exploitation material offences: Characteristics of offenders and an exploration of judicial censure. Psychiatry, Psychology and Law, 27(4), 647–664.

Colley, S. (2019). Perpetrators of organised child sexual exploitation (CSE) in the UK: A review of current research. Journal of Sexual Aggression, 25(3), 258–274.

Cullen, O., Ernst, K. Z., Dawes, N., Binford, W., & Dimitropoulos, G. (2020). "Our laws have not caught up with the technology": Understanding challenges and facilitators in investigating and prosecuting child sexual abuse materials in the United States. Laws, 9(4), 28.

Demetis, D., & Kietzmann, J. (2021). Online child sexual exploitation: A new MIS challenge. Journal of the Association for Information Systems, 22(1), 9.

ECPAT. (2016). Terminology guidelines for the protection of children from sexual exploitation and sexual abuse. Bangkok: Every Child Protected against Trafficking (ECPAT) International.

ECPAT. (2017). Online child sexual exploitation: An analysis of emerging and selected issues. ECPAT International Journal, 12, 1–63. http://ecpat.de/wp-content/uploads/2018/08/Journal_No12-ebook.pdf

ECPAT. (2018). Trends in online child sexual abuse material. Bangkok: Every Child Protected against Trafficking (ECPAT) International.

Franchino-Olsen, H. (2021). Vulnerabilities relevant for commercial sexual exploitation of children/domestic minor sex trafficking: A systematic review of risk factors. Trauma, Violence, and Abuse, 22(1), 99–111.

Gabel, S. G. (2012). Social protection and children in developing countries. Children and Youth Services Review, 34(3), 537–545.

Gill, M. (2021). Online child sexual exploitation in the Philippines: Moving beyond the current discourse and approach. Anti-Trafficking Review, (16), 150–155.

International Justice Mission. (2020). Online sexual exploitation of children in the Philippines: Analysis and recommendations for governments, industry and civil society. International Justice Mission. https://ijmstoragelive.blob.core.windows.net/ijmna/documents/studies/Final-Public-Full-Report-5_20_2020.pdf

Joleby, M., Lunde, C., Landström, S., & Jonsson, L. S. (2021). Offender strategies for engaging children in online sexual activity. Child Abuse and Neglect, 120, 105214.

Kloess, J.A., Beech, A.R., & Harkins, L. (2014). Online child sexual exploitation: Prevalence, process, and offender characteristics. Trauma, Violence, and Abuse, 15(2), 126–139.

Krone, T., Smith, R.G., Cartwright, J., Hutchings, A., Tomison, A., & Napier, S. (2017). Online child sexual exploitation offenders: A study of Australian law enforcement data. Criminology Research Grants, 77, 1213.

Laird, J.J., Klettke, B., Hall, K., & Hallford, D. (2023). Toward a global definition and understanding of child sexual exploitation: The development of a conceptual model. Trauma, Violence, and Abuse, 24(4), 2243–2264.

Long, J. S. (2023). Sexual exploitation and sexual abuse of children. In: D. Hummer and J. Byrne, Handbook on Crime and Technology (pp. 251–277). Edward Elgar Publishing.

Myers, W., & Bourdillon, M. (2012). Concluding reflections: How might we really protect children? Development in practice, 22(4), 613–620.

Ramiro, L.S., Martinez, A.B., Tan, J.R.D., Mariano, K., Miranda, G.M.J., & Bautista, G. (2019). Online child sexual exploitation and abuse: A community diagnosis using the social norms theory. Child Abuse and Neglect, 96, 104080.

Ringenberg, T.R., Seigfried-Spellar, K.C., Rayz, J.M., & Rogers, M.K. (2022). A scoping review of child grooming strategies: Pre-and post-internet. Child Abuse and Neglect, 123, 105392.

Roche, S., Otarra, C., Fell, I., Torres, C.B., & Rees, S. (2023). Online sexual exploitation of children in the Philippines: A scoping review. Children and Youth Services Review, 148, 106861.

Simon, J., Luetzow, A., & Conte, J. R. (2020). Thirty years of the convention on the rights of the child: Developments in child sexual abuse and exploitation. Child Abuse and Neglect, 110, 104399.

Toro Quezada, E.P. (2018). Analysis of policy and legal frameworks, intervention models and intervention practices on commercial sexual exploitation of children in Chile: A discourse analysis approach. Thesis, University of Edinburgh.

Tripathy, J. P. (2013). Secondary data analysis: Ethical issues and challenges. Iranian journal of public health, 42(12), 1478.

United Nations Office on Drugs and Crime. (2020). Online child sexual exploitation and abuse [online]. United Nations Office on Drugs and Crime (UNDOC). https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html (accessed 20 May 2024).

## Study H: Access denied

Hunter, P. (2004). BT's bold pioneering child porn block wins plaudits amid Internet censorship concerns. Computer Fraud and Security, 2004(9), 4–5. https://doi.org/10.1016/S1361-3723(04)00109-5

## Additional reading

Brown, I. (2013). Research handbook on governance of the internet (1st ed.). Edward Elgar Publishing, pp. 1–499. https://doi.org/10.4337/9781849805049

Kantas, E., & Dekker, M. (2022). Security and privacy of public DNS resolvers. European Union Agency for Cybersecurity (ENISA) Publications Office.

Parti, K., & Marin, L. (2013). Ensuring freedoms and protecting rights in the governance of the internet: A comparative analysis on blocking measures and internet providers' removal of illegal internet content. Journal of Contemporary European Research, 9(1), 138–159. https://doi.org/10.30950/jcer.v9i1.455

Singh Grewal, S. (2011). New hotline on blocked websites. In: McClatchy – Tribune Business News. Tribune Content Agency LLC.

Varadharajan, V. (2010). Internet filtering – Issues and challenges. In: IEEE Security and Privacy (Vol. 8, No. 4, pp. 62–65). IEEE. https://doi.org/10.1109/MSP.2010.131

CHILDLIGHT

Global Child Safety Institute

## Contact us

childlight@ed.ac.uk

## Follow Us

𝕏 @ChildLight_

in Childlight –
Global Child Safety Institute

Find out more