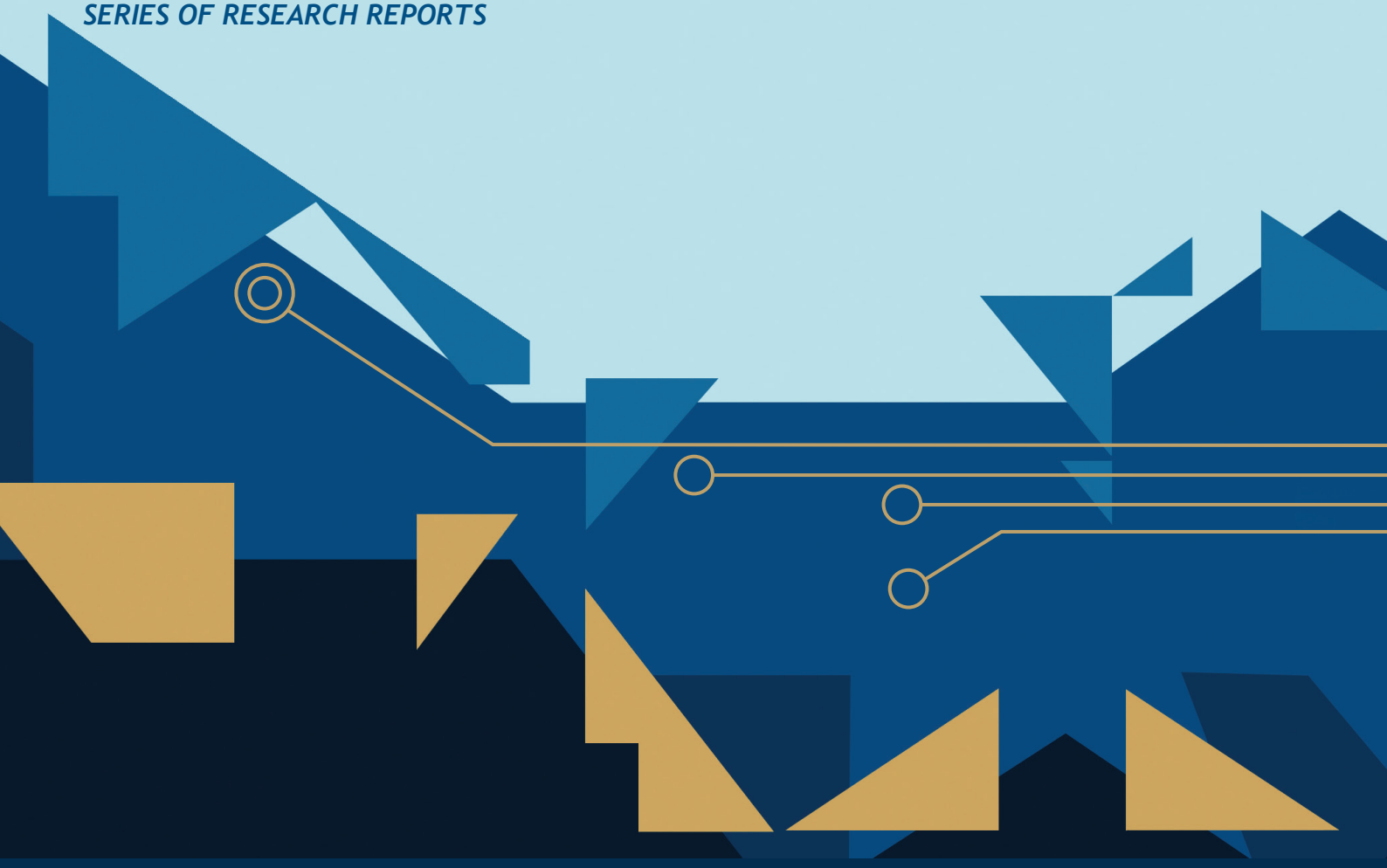
Child Sexual Abuse on the Internet

Report on the analysis of technological factors that affect the creation and sharing of child sexual abuse material on the Internet.

Matilda Dorotic and Jan William Johnsen

No. 1 - 2023
SERIES OF RESEARCH REPORTS



BI Norwegian Business School

NTNU

Matilda Dorotic og Jan William Johnsen
Child Sexual Abuse on the Internet. Report on the analysis of technological factors that affect the creation and sharing of child sexual abuse material on the Internet

Research Report
1 edition
1 reprint
ISSN: 0803-2610

BI Norwegian Business School
N-0442 Oslo
Phone +47 4641 0000
www.bi.no

Child Sexual Abuse on the Internet

Report on the analysis of technological factors that affect the creation and sharing of child sexual abuse material on the Internet

Project manager
Basel Katt

Authors of the report
Matilda Dorotic and Jan William Johnsen

Data sourcing
Patrick Bours and Marius Wang

Formatting
Oliver Dagsland Tverrå

Content

Acknowledgments

This research received funding from the Norwegian Ministry of Justice and Public Security through *SOBI Del III: Kartlegging og analyse av arenaer som brukes til tilgang og deling av overgrepsmateriale*.

We want to thank our partner Trøndelag police district, superintendent Marius Wang, for providing the data necessary for this research and for facilitating interviews with specialized investigators. We are grateful for the support of our partners at the Norwegian National Criminal Investigation Service (Kripos), Celina Røstgård Flatner, and at Oslo police district, Bente Skattør, for their insight and support in data collection and for facilitating interviews with police officers and investigators.

Important contributions were made by firms, civil society organizations and individuals, as they kindly collaborated with us on interviews and provided information and context for the development of a multistakeholder perspective. To keep the anonymity of our interviewees, we have refrained from mentioning the names of firms and institutions that participated in this research, but hereby thank them collectively.

We are grateful to civilian organizations that provided important insight into the multistakeholder challenges: Redd Barna, part of the Save the Children organization (Kaja Hegg) and Amnesty International Norway (Ingrid Westgaard Stolpestad). We are grateful to United Nations Interregional and Norwegian Data Protection Agency (Datatilsynet) for insightful comments that they have provided to this report.

Finally, we want to thank Professor Katrin Franke at the Norwegian University of Science and Technology (NTNU) for her efforts in researching and writing the proposal which was the starting points for this research.

Foreword

Technological developments, particularly those related to electronic services used on the internet and through artificial intelligence (AI) advancements, have brought important benefits in fostering communication, access to information and sharing. However, these advancements have also brought significant challenges to making online environments safe for children while protecting privacy and freedom of speech. This report sheds light on the complex role that technology plays in the creation and sharing of online sexual abuse materials and the critical role of technology in creating counter solutions to detect and prevent abuse.

On the one hand, the efforts by the postal services to combat the distribution of child abuse material via mail services were successful in the 1990s in reducing the offline sharing of child sexual abuse material (CSAM) [1], [2]. However, the creation and sharing of online CSAM surged across the globe with the development of the internet and electronic services [3], [4]. In the period from 2005 to 2020, there was a 15,000% increase in the number of abuse files reported to the global CSAM clearinghouse, further increasing by 35% between 2020 and 2021 [6]. The widespread use of mobile devices and accessibility of online services and platforms that enable instant communication, video streaming and massive sharing of materials enable offenders to easily contact multiple victims and buy, sell, and exchange illicit images and videos in the privacy of their home. Moreover, the increased development of anonymization techniques (such as end-to-end encryption or dark web services) and new forms of artificially created imagery make abuse and CSAM more difficult to detect and remove.

On the other hand, the sheer volume of abuse material online and the rate at which the new content is created make manual review impossible and require the use of technological solutions and close private–public partnerships between electronic service providers and other stakeholders (parents, civil society, governments, and law enforcement). Hence, technological developments paradoxically play a role in both aiding and counteracting the problem.

Due to the complex nature of drivers, harms and structures that facilitate these trends, law enforcement cannot approach these problems alone or in isolation. The detection and prevention of online sexual abuse of children represents a nuanced and complex phenomenon to investigate because it is characterized by a multiplicity of stakeholders. Although all stakeholders agree that this problem represents an important social issue, achieving one stakeholder's goals (e.g., allowing law enforcement to increase its surveillance of the internet) directly impacts the rights and abilities of other stakeholders (e.g., intrusion in the privacy of individuals or infringement of electronic service providers on client-service relationships). The need to increase awareness and education about the perils of self-generating illicit imagery, the social norms that prevent a wider discourse on the topic and a clash of opinions about how to approach the solutions between those who support stronger governmental surveillance and those who oppose it constitute heated elements in the current debate.

We hope this work will contribute to a better understanding of the complexity surrounding the issue and help in creating a single policy framework for a safer and better internet for children.

Chapter 1: Introduction

1.1 Purpose and aims of the report

Online child sexual abuse (CSA) has increased rapidly in the last three years since the start of the COVID-19 pandemic, driven by children's wider access to the internet but also by rapid technological advancements. The number of reports about online images, videos and other forms of child sexual abuse materials (CSAM) submitted by the public and firms to the US Cyber Tipline surged from approximately 1 million in 2010 to 16.9 million in 2019 and 29.3 million in 2021 [6].

The threats to children and other groups at risk in online environments have become a major social issue around the globe, becoming major national and international strategic priorities for legislators in the US, Norway and the European Union [7] (cf. Norwegian National Strategy for Coordinate Efforts; European Strategy for a Better Internet for Kids (BIK+) and Communication Decency Act's discussions in the US).

Almost universal rates of access to the internet and mobile devices in European countries, including Norway, make children increasingly adept at technological advances and connected to online content. However, high levels of internet access also expose children to increased internet-related threats and abuse, particularly through the consumption, creation or sharing of abusive materials; children have also been harmed through grooming (i.e., befriending children online through gaming or social media platforms with the intent to sexually exploit them). Moreover, children's widespread use of mobile devices and the time they spend on the internet have moved their social interactions largely online, increasing the rate at which they self-generate illicit imagery and share this materials with other minors; moreover, the boundaries minors faced in sharing explicit content have deteriorated. The age limit has decreased, and almost 7 in 10 instances of identified online CSAM by the internet Watch Foundation (IWF) in 2021 involved 11- to 13-year-olds [8]. More than half of Norwegian teenagers between 13 and 18 years of age indicate that they have been asked to share naked photos of themselves [9].

The rapid development of digital solutions that facilitate interactions with (and among) children has increased the sources of harm and made it harder to identify perpetrators [10]. Online abuse represents a specific type of harm that is frequently perpetrated through social sharing and stems from a lack of awareness. It is particularly detrimental to youth because abusive materials remain online, and the continuous sharing of the material revictimizes children repeatedly. 70% of CSAM victims indicated that they constantly worry that they may be recognized by someone who has seen the material [11].

Regulators, law enforcement, civil society organizations, and parents have raised strong concerns about online safety for children and called for immediate action. However, the prevention of harm to children has suffered from several important tensions that have made prevention efforts particularly cumbersome:

- Inadequate technological skills in parents, educators, and law enforcement officers.
- Legal ambiguities because technology develops faster than legislation.
- Infringement on privacy and human rights.

- Provision of commercial confidentiality of user information by service providers.
- Technology providers' need to protect their intellectual property rights.
- Lack of transparency and biases in artificial intelligence (AI) algorithms.

In particular, one of the most important issues that has hampered prevention and detection efforts is the global nature of the internet, which demands that legal frameworks must be harmonized across countries for the implementation of global prevention actions. However, this harmonization has not taken place; indeed, there are different legislations with some countries mandating the reporting of CSAM, others making this reporting voluntary and more than half of the countries worldwide still not having laws related to CSAM [5] [28]. Over 60% of child sexual abuse material worldwide is hosted on European servers [12] because of the lack of regulatory conditions in Europe (unlike in the US) for mandatory reporting of CSAM by electronic service providers. New regulatory proposals in the EU and UK (e.g., BIK+ and Online Safety Bills) aim to change the legislation and reduce the favorable conditions for storage and dissemination of online CSAM in Europe [7]. These processes directly affect the future of Norwegian law enforcement practices and the ability to prevent harm to children and youth in Norway. According to the BIK Policy Map profile from March 2021, Norway does not have a single coordinated policy framework on the subject of child safety on the internet, nor any initiatives to implement standards for quality online content for children, initiatives on cooperation between law enforcement and helplines or initiatives to monitor reporting mechanisms or codes of conduct at the national level [7].

This report contributes toward the national strategy goals of ensuring that children and young people are safe on the internet through an evaluation of technological arenas, channels and trends that affect the online sexual abuse and exploitation of children [13]. Toward this end, this report addresses three main research issues:

- How the development of digital technology and services impacts a) the possibilities for access and sharing of child sexual abuse materials (CSAM) and b) the possibilities for perpetrators to establish contact;
- The most prominent current and future technological trends; and
- The technical and other possibilities (structural, legal) that exist to combat these issues.

We hope that this report will inform and facilitate national strategy building efforts.

1.2 Structure of the report

Creating efficient strategies and policies for the detection and prevention of online abuse requires knowledge of the arenas that enable and facilitate such abuse, as well as of the stakes of the diverse stakeholders and the pitfalls they meet in working together toward those goals. Since the ability to implement methods to reduce online CSA inevitably depends on cooperation and coordination between multiple stakeholders, our evaluation aims to be holistic and include the perspectives of multiple stakeholders to highlight their interdependence. Nevertheless, the main focus of this report is on the ways in which technology impacts the creation, sharing and prevention of online child sexual abuse.

Given the complexity and multiplicity of different technological solutions, we inevitably had to focus our attention on only the most prominent aspects and cover other related aspects more superficially (e.g., the legal conditions, business environment aspects, and social side of the CSA).

In this first chapter, this report starts by outlining the methodological approach taken and its limitations and familiarizing the reader with the main terminology used in the report. The second chapter outlines the main types and sources of online sexual abuse of children, focusing predominantly on the creation of CSAM. Our aim is to compile in one place a comprehensive picture of the main formats and sources of CSA in the face of the diversity and variability of the sources and terms used sporadically in the literature. In the third chapter, the report outlines existing countermeasures implemented by law enforcement, as well as the reported trends and pitfalls that law enforcement encounters in this area. The final, fourth chapter covers structural and legal challenges in the prevention of CSAM, and we highlight the relevant aspects and drawbacks identified by various stakeholders. Our explanations in the fourth chapter are based on insights from civil society groups', firms' and legislators' reports about the challenges they meet and the trade-offs they make. Throughout the report, we provide a balanced, independent assessment and recommendations on the potential aspects to consider in designing future policies to make children safe in online environments.

1.3 Method

Given the previously described complexity of the phenomena and interrelated issues among multiple stakeholders, we adopted a multimethod approach for our analysis, in which we combined a literature review of desk-research evidence (both from public records and academic sources) with an analysis of available empirical evidence from national and regional crime prevention units and primary data collection through interviews with main stakeholders.

The literature review focused primarily on technological trends and countermeasure solutions. The initial analysis of the Web of Science repository of peer-reviewed papers in the domains of computer science, criminology, forensics and psychiatry using the topical keywords "child sexual abuse", "CSA", "CSAM" and "child pornography" resulted in 18528 references, with most papers emanating from psychology and psychiatry, family studies and social work. An analysis of those papers showed that the vast majority of those studies did not examine the technological aspects. Often, these studies analyzed court records to understand the profile and characteristics of offenders or social work datasets and surveys of victims to understand what these perceived. This lack of studies led to the snowball sampling of first publicly available reports from organizations addressing children's protection (The International Centre for Missing & Exploited Children (ICMEC), NCMEC, INHope, WePROTECT Global Alliance, UNICEF, INTERPOL, etc.) as well as governmental reports on CSAM strategies that had been employed or discussed. As this review revealed the need to access studies in law, computer science and social science, we used the references noted in those studies to conducted an additional snowball sampling of the academic literature. Consequently, with increased the number of peer-reviewed sources through the snowball sampling of reports and open-source findings via Google Scholar analysis, and we explored approximately 125 sources referenced in this study. To be included in our review, papers had to be

academically rigorous and sound (based on the ranking of the scientific journals and conferences in which these papers appeared), and the NGOs had to be credible in the children's protection sector. When including reports, we focused on the leading NGOs and legislative repositories. In addition, we complemented the analysis by evaluating the transparency reports included in the largest electronic service providers reporting to NCMEC (the analysis included transparency reports from Meta, Google, Tik Tok, Microsoft, Dropbox, Snapchat, Twitter, Imgur and Reddit).

To complement the literature survey with empirical data, we enhanced our analysis by including police reports and in-depth interviews with stakeholders from law enforcement, legislators, civil organizations representing children, nonprofit organizations catering to parents and children, and firms. We conducted a series of 16 interviews and work-session meetings to obtain in-depth insights on issues from a multistakeholder perspective. Firms' representatives from various electronic service providers were included (online gaming, financial institutions, communication, and software services). The stakeholders' names were anonymized to protect the privacy of individuals and organizations.

Overall, we interviewed sixteen (16) respondents: we produced eight in-depth interviews with respondents from diverse levels in the Norwegian law enforcement hierarchy (national level investigators, district level investigators, police officers, and first respondents); three interviews with regulators and civil society/children's rights experts; and five interviews with representatives from the business sector.

To collect data for this report, we conducted an analysis of aggregated empirical evidence obtained from Norwegian law enforcement and Kripos. We also used the aggregation of materials to represent a particular issue whenever possible. No personal data were accessed in the course of this study.

1.4 Limitations

Due to the complexity of the aspects related to the online abuse of children, we had to be restrictive in our scope, and at times we were limited in the aspects we could include. In the final version of the report, we had to exclude certain aspects for the sake of brevity. Therefore, the report is inevitably not exhaustive in the way it addresses diverse aspects, but it rather aims to highlight some main aspects and links those aspects we deem to be the most relevant to an understanding of the impact of technology. The geographical focus of the analysis is limited to the aspects and practices relevant to Norway in particular, although some related aspects also pertain to the US and the EU. It is generally difficulty to provide a systematic literature review on the impact of technology on CSA, because this literature is fragmented across different academic disciplines focusing on narrow aspects , and the technology papers focus on a specific technology; overall, there is a lack of large-scale empirical studies. This limitation in data sources makes the analysis across studies difficult and limits any ability to provide large-scale empirical generalizations. In particular, to analyze volumes, scopes and trends, we predominantly had to rely on annual reports from a few major NGOs in the field (NCMEC, IWF and InHope) and transparency reports from a few large ESPs, whose limitations in providing the overall state of the field are elaborated in Section 2.2.

Some of the figures and data obtained from police sources cannot fully distinguish sexual abuse harms perpetrated online or offline due to weaknesses in the existing penal code, which does not account for locations and technologies used. Moreover, given that much of the offences are still classified manually by numerous police officers and that there is no consistent approach to the writing of annotations, the interpretation of our findings may be obscured.

Finally, we have attempted to provide an objective assessment of the academic literature and obtained materials from the field; however, the interpretations and all potential errors or inaccuracies in this report are the authors' own. The project's partners, institutions, law enforcement agencies and interviewed individuals are not responsible for the interpretation of the content.

1.5 Terminology

There is no internationally and uniformly agreed upon definition or terminology for online child exploitation and abuse. UNICEF has warned that the term often includes various forms of technology-facilitated child sexual exploitation and abuse [5].

Child abuse and exploitation (CAE) comes in many forms, such as child prostitution and exploitation, direct sexual abuse, grooming or sharing materials. These crimes can occur both online and offline. This report focuses particularly on *online child sexual exploitation and abuse*, which UNICEF refers to as "technology-facilitated child sexual exploitation and abuse" that is partly or entirely facilitated by technology, either through the internet or other wireless communications channels [5].

For the purpose of this report, we use the definition of child sexual exploitation and abuse adopted by the Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention), Article 18.

Child sexual abuse (CSA) is defined by activities in several domains:

- engaging in sexual activities with an underage person;
- production, possession and distribution of child sexual abuse material (CSAM);
- grooming of potential child victims online with the intention of sexual exploitation, or
- live streaming of child sexual exploitation and abuse.

The distinction between abuse and exploitation refers primarily to the nature of exchange [5]. If a second party benefits financially from the activities, child sexual abuse becomes sexual exploitation. In this report, we use the abbreviations CSA and CSAM in their broad sense to encompass any type of abuse or exploitation.

Child sexual abuse material (CSAM) encompasses content produced in various formats (most often images, videos and livestreaming) that is shared via digital channels.

Electronic service provider (ESP) or internet service provider (ISP) refers to a business that provides digital communication services that allow receiving and transmitting information through electronic channels (notably the internet). For the purpose of this report, we use the term ESP to broadly refer to

various information technology companies, including telecommunication service providers and online digital service providers (e.g., digital platforms used for entertainment [gaming], social media providers, etc.)

Grooming refers to the activities of groomers, i.e., individuals who seek to build online relationships with children and convince them to send nude pictures or explicit videos or who engage in sexual activities as part of the grooming process. By doing so, they can deceive or coerce children into CSA. The perpetrator often poses as someone else, e.g., someone the same age as the child, using one or more false profiles [14]. The perpetrator has often created additional profiles to give the child the impression that several persons vouch for the main profile. The perpetrator exhibits considerable insight into how children and young people talk and communicate, which allows him or her to communicate with children in a credible manner.

An **IP address** is an abbreviation for an internet protocol address; it is a numerical label (e.g., 192.0.2.1) that identifies a computer or network that uses the internet protocol for communication [15]. Both the sender's and the recipient's IP addresses are needed to send data packages on the internet. An IP address is allocated to the customer’s computer equipment by the internet service provider [14] and can be used for network interface identification and location addressing.

The Open Web consists of information on the internet (i.e., the Worldwide Web) that can be indexed by regular search engines and that appears in the results of searches on search engines such as Google, Bing, Yahoo, and Firefox.

The dark web (or darknet) consists of encrypted networks that encode information in such a way that it cannot be indexed by regular search engines [16]. The darknet encryption technology routes users' data through a large number of intermediate servers, which hide the users' identity. Through the dark web, private computer networks can communicate and conduct business anonymously without divulging identifying information, such as a users’ location. Accessing the dark web also requires special browsers or software such as The Onion Router (TOR).

Cryptocurrency (often synonymous with bitcoin) is a term referring to a *digitized asset* spread through multiple computers in a shared network [17], which can be used as an alternative digital payment currency. Given that cryptocurrency is shared through decentralized networks, it cannot be directly controlled by governments’ regulatory bodies (such as banking systems).

Chapter 2: Sources and channels for the online sexual abuse of children

2.1 Overview of technological developments in the proliferation of online CSAM from the 1990s to 2021

The distribution of CSAM via official postal services (an offline channel) was in decline before the appearance of the internet in the 1990s [1] [18]. Initially, online CSAM was mostly shared through communication systems such as email or direct messaging via applications and websites. Between 1996 and 2004, most offenders visited websites to host and access CSAM images [2] and to share URL links of material stored by file hosting services [19]. The broad dissemination of CSAM did not start before the development of new file sharing technologies between 2004 and 2008, such as peer-to-peer (P2P) server systems and BitTorrent software. P2P links offenders in decentralized networks that allow them to download multiple files and share them with other peers (i.e., users) [2] [20]. The amount of available CSAM continued to grow during this period.

Between 2008 and 2014, offenders became increasingly anonymous through the use of cryptocurrencies, virtual private networks (VPNs), and Tor (hidden service) networks. Since 2014,the context has been defined by the widespread use of mobile technology, both for the creation and sharing of materials [2]. Mobile technology has made the production, distribution, sharing and consumption of CSAM easier because of factors such as inexpensive data plans, high-quality mobile screens and cameras, and the wide availability of streaming and recording applications. Devices such as tablets and smartphones have been increasingly used to disseminate CSAM, and they made up 32% of all queries associated with CSAM on Microsoft's search engine Bing in 2015 [21].

Mobile devices continue to have an important impact. A 2021 report showed that 62% of young respondents who received sexually explicit material had received it on their mobile device [22]. Mobile technology has driven the increase in video and live streaming of online CSA. The increase in mobile use has also increased the risk that younger children be abused. A particular factor influencing this trend is that there has been more self-produced amateur content [23] (see also Subsection 2.3.2).

The widespread adoption of the internet and social media, combined with easy access to computers, tablets, and other mobile devices for children and young people, has created major opportunities for offenders seeking to establish sexual contact with them [1] [2]. The development of the internet and related digital services has facilitated three factors in online abuse:

i) Wide and easy access to online materials facilitating and normalizing the sharing of material,
ii) Increased ability of perpetrators to target multiple victims at the same time and orchestrate the abuse in real time, and
iii) Offenders' increased ability to hide their identity due to the great possibility for anonymization and the ability to easily create multiple accounts.

Technological advancements continue to challenge law enforcement's ability to prevent, investigate and prosecute online child sexual exploitation and abuse. Offenders utilize technology to obtain and view material in new ways, hide their activities and act in ways that counter the protection of children [24].

Among recent trends, we note that offenders have increasingly used end-to-end encryption and the dark web to protect the privacy of their communication, whether through online messaging services or mobile devices in general, which in turn has had the potential to further increase offenders' anonymity and decrease the chances of identifying and sanctioning CSA. Moreover, novel forms of CSAM production, distribution, and consumption have been on the rise. For example, artificially generated CSAM has challenged the ability to identify victims and offenders and allowed for new forms of CSAM that were previously unknown to be created (e.g., via extended reality and deepfake). To better understand this complexity, in the next sections of this report, we provide an outline of the different formats, sources and technology-enabled distribution channels that facilitate online CSA.

2.2 Scope of the Problem

Limitations to the understanding of the full scale of the volume of CSAM

The true extent of the spread and actual volume of CSAM has been difficult to track and evaluate; indeed, this scope is impossible to assess due to the potentially large volume of undetected CSAM. Several obstacles make the full volume of CSA and CSAM difficult to estimate. First, part of this CSAM is inaccessible to the general public and even to electronic service providers (ESPs) because it is produced and shared through encrypted networks or proprietary digital services through which only the senders and receivers can see messages. Second, the sheer volume of online material makes screening and tracking difficult even for open web and networks. With more than one million hours of streaming produced every minute worldwide, 16 million texts shared, approximately 5.9 million searches on Google, 2.4 million snaps on Snapchat and 1.7 million content pieces shared via Facebook, identifying and processing abusive content has become a major challenge for ESPs [126]. The vast volume as well as the various technologies employed have made it difficult for law enforcement and NGOs to track the dissemination of CSAM. The third obstacle comes from the fact that available information on detected CSAM is fragmented across different NGOs and ESPs, and the measures these entities employ individually are not directly comparable. For instance, the largest global source of reported CSAM comes from the National Center for Missing & Exploited Children (NCMEC), to which US-based ESPs (such as Meta, Google, etc.) have a duty to report detected CSAM on their services, according to US federal law. Conversely, in Europe and the United Kingdom, where at the moment there is no legal obligatory reporting requirement, the detection of CSAM relies on tips from the NCMEC and local hotlines, which receive reports from the public or ESPs, which themselves can tag or report URLs, images or videos found online that contain CSAM (the main European hotline networks are InHope in the EU and internet Watch Foundation in the UK).

We attempted to gain an understanding of the efficiency of the current systems in assessing the full volume of CSAM by analyzing transparency reports made by ESPs and reports from clearinghouses and hotlines; hence, we evaluated the efficiency of public reporting versus identification of CSAM by ESPs through their internal systems [25]. The NCMEC reported that in 2021, more than 99% of reports came from ESPs rather than from the general public (ESPs reported over 29.1 million out of 29.3 million reports in total) [6]. In turn, transparency reports from Meta and specifically the Facebook’s Community

Standards Enforcement Report concerning child endangerment have shown that as much as 99% of all reported materials are detected proactively through the use of ESPs' internal software solutions, while only 1% of all reports come from public reports/users [26]. Similar percentages are reported by Microsoft, Google, Snap, Twitter and other providers [25]. These findings illustrate that relying on public reporting of available CSAM is inefficient. This analysis shows that the diligence of ESPs in detecting and removing CSA online and the legal enforcement of the requirement that ESPs detect and report CSA play a crucial and necessary role in curbing the social problem of online CSA. However, watchdog organizations and parents who voluntarily survey and report abuse online on popular social media platforms have raised criticisms and warned about faulty algorithms and the ease with which CSAM perpetrators can avoid detection by internal systems even when ESPs are diligent [72].

Furthermore, the system of voluntary reporting by ESPs and the lack of global legal requirements for ESPs to actively scan and search for CSA and CSAM in their services have resulted in an inconsistent and sporadic detection of CSAM, which is typically undertaken by the few largest technological ESPs and is missing for hosts of other ESPs (particularly among smaller and mid-size firms). Concretely, the NCMEC has reported that as much as 93% of all reports come from one provider—Meta (which owns Facebook, WhatsApp and Instagram) [6]. The NCMEC's services were accessed by 1400 providers all together, while many more exist in the US. The IWF, the main UK's hotline, has identified 175 companies (within the UK and globally) currently working with the foundation's member services [8], in comparison to the more than 351,000 ICT businesses registered in the UK in 2017—a number likely to be greater today. Moreover, the IWF has reported that as much as 66% of all contents assessed and 94% of actions against perpetrators were sourced proactively by their own analysts who searched the internet rather than sourced from external reports by the public, police, hotlines and ESPs [8].

In conclusion, due to the differences in regulatory frameworks, an inability to account for the full spectrum of online services through which CSAM may be produced or shared and the vast amounts of content being continuously uploaded, our analysis led us to believe that the amount of undetected CSAM that circulates online is substantively larger than the numbers we have been able to uncover.

Against this backdrop and outlined limitations, we further discuss the numbers and trends that have been retrieved through our analysis of the literature and primary evidence from Norwegian law enforcement.

Volume and global trends in CSAM based on reports to clearinghouses and hotlines

The main way in which the trends in CSA are estimated relies on the number of tips (reports) that the hotlines and clearinghouse receive. Overall, since its inception in 1998, the NCMEC has reported receiving over 82 million reports about different forms of child sexual abuse materials found online, and it has reviewed over 322 million images and videos and identified over 19,100 victims in collaboration with law enforcement [29]. In 2021 alone, the NCMEC's Cyber Tipline received 29.3 million reports, of which 99% fit in the CSAM category and 1% referred to other forms of CSA (such as online enticement, grooming, sex trafficking, etc.) [29]. The number of reports has increased over time; for example, in

2021, that number increased by 35% relative to 2020 [29]. The European network of hotlines, InHope, has reported receiving 928,278 content URLs of potentially illegal and harmful material depicting child sexual abuse and exploitation in 2021 (each URL may contain multiple images or videos). In 2021, the Internet Watch Foundation (IWF) assessed 361,062 reports of URLs, out of which 7 in 10 (252,194 reports) led to the finding of online imagery in which children were being sexually abused [8]. The IWF recorded an increase of 20% in the number of reports in 2021 relative to 2020 [8]. As our overview illustrates, the difference in reporting numbers between the NCMEC and other hotlines has been substantial, which may reflect the fact that US-based ESPs are much larger but may also reflect the differences in reporting system requirements that exist in different countries as well as the lack of laws in this domain globally. Since reporting can be done per website (with multiple cases) or on a single image/file and because the same material can be tagged by more than one person, ESP or report, a direct comparison across hotlines is not useful. Therefore, we analyzed the number of unique (nonrepeating) materials reported by clearinghouses and the number of reports that were confirmed to contain CSAM. According to the NCMEC's reports, in 2021, approximately 42% of all reported images were unique (16.9 million out of 39.9 million images), and 11% of reported videos were unique (5.1 million out of 44.8 million) [29]. Approximately 70% of IWF reports were confirmed to contain CSAM, and approximately 13% of the reports made by the public have been actionable (confirmed to contain CSAM) [8]. Finally, InHope reported that 82% of contents/URLs that were analyzed in 2021 were unknown [to their database] [30]. It is unclear how many of those images are unique or constitute new images or potentially overlap with sources identified by the NCMEC or other hotlines.

Together, these numbers show that even in the strictest view of the reported and confirmed sources, the number of CSAM per year amounts to tens of millions and that the number of reports has increased in recent years at a rate of between 20 to 30%; moreover, the most significant source of detection of CSAM is the proactive search by ESPs and NGOs rather than a retroactive tagging or tips from the public (which seem to be less reliable in terms of accuracy but more sporadic and negligible in terms of their overall volume).

Overview of CSA and CSAM trends in Norway

After looking at the global numbers and trends, we provide the share of CSA cases reported in Norway, looking at trends reported by Norwegian law enforcement as well as the volume of cases obtained from the clearinghouse (NCMEC), which represents the main external source of reports.

Figure 1 illustrates trends in the number of CSA-related police cases in Norway in the period from 2017 to 2021. Although the number of cases registered by the police in relation to CSA in Norway has varied slightly over the years, we see an overall increase in the number of cases over time (reaching a record 4417 cases in 2021). Importantly, the current Norwegian Penal code registry does not allow for the distinction between offline and online cases of CSA, and it lacks clear guidance for the registration of offenses in the system; indeed, various operators register offenses inconsistently. Therefore, these statistics may not give a clear picture allowing a comparison of trends in online CSAM and CSA.

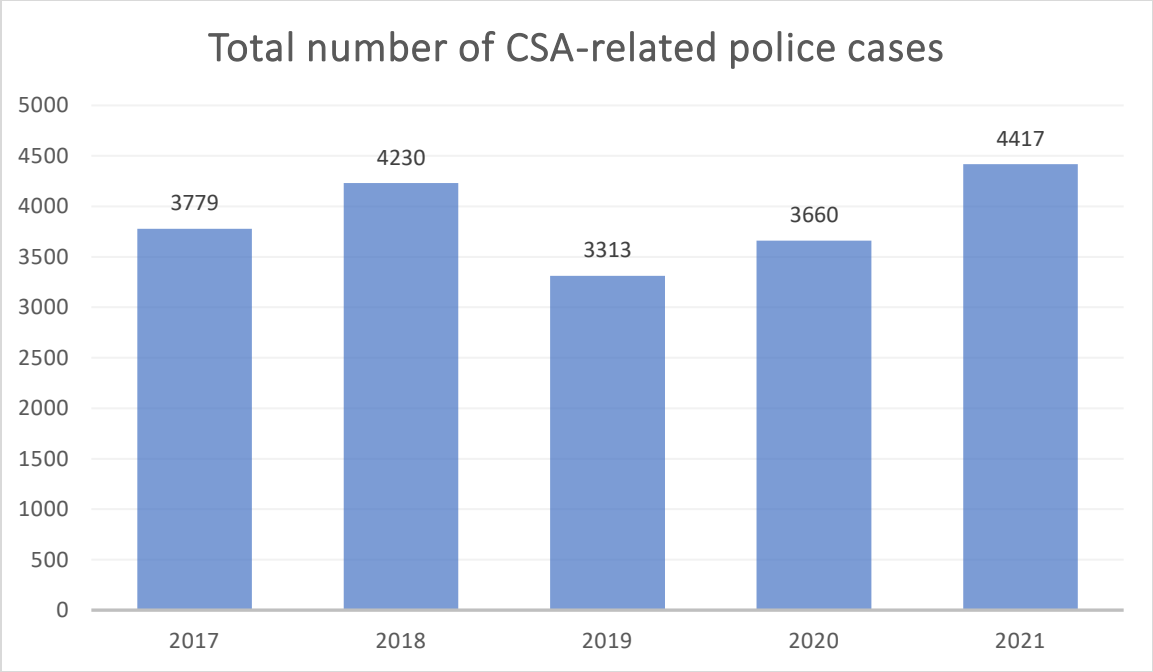


Figure 1: Total number of police cases related to any aspect of CSA across all police districts in Norway. Source: Data obtained from the Norwegian registry of offences (STRASAK).

To better understand online CSA cases, we explored the main external reporting source of online CSAM concerning Norwegian citizens and IP addresses, which emanates from the NCMEC. The reports made by the NCMEC are sent to the Norwegian National Criminal Investigation Service (Kripos), which then further distributes the reported cases to regional police districts. Table 1 indicates the CSAM reports that Norwegian law enforcement obtained from the NCMEC. In 2021, Norway received approximately 7850 reports out of the total number of reports received by the NCMEC. The NCMEC has shown that reports have been distributed across countries, with the largest number of reports coming from India, the Philippines and Pakistan [6], countries with a much larger overall population and less developed legal systems compared to Norway; therefore, the fact that a relatively small percentage (less than 1%) of global reports is related to Norway is understandable.

	2018	2019	2020	2021
Number of NCMEC reports globally*		16 987 361	21 751 085	29 397 681
Number of NCMEC reports to Norway	10 463	6 868	7 039	7 850
Reports implemented for further analysis	1 468	1 928	2 549	3 644
Percentage of imported cases	14.0%	28.1%	36.2%	46.4%

*Table 1: Overview showing the number of reports received from the NCMEC organization by Norwegian law enforcement. Source: Kripos, NC3 unit (2022). Statistikk fra Seksjon for internettrelaterte overgrep - behandling av NCMEC. *Statistics from NCMEC website: NCMEC Data (missingkids.org).*

An in-depth discussion with law enforcement officers about the interpretation of trends in the NCMEC reporting shows that the decline in the number of cases reported between 2018 and 2019 is not an indicator of a lower level of abuse in Norway. Instead, it reflects the fact that implementation of end-to-end encryption in some services (e.g., WhatsApp, Skype and Snapchat) and the shutting down of Yahoo Messenger caused a drop in the number of NCMEC reports in 2018-2019 [cf. also 25].

In recent years, new AI tools employed by the NCMEC have become more effective, which has led to the better identification of actual cases and a reduction in false positives (wrongly labeling an image or video material as illicit). This development has relied on the fact that the percentage of imported cases (percentage of cases that were selected for further criminal investigation) has increased from 14% in 2018 to 36.2% in 2020 and 46.4% in 2021. The *number of reports subjected to further analysis* in Table 1 represents reports that have been manually inserted in the crime handling database. To insert a case in the database, there must be a clear indication that the facts of the case are in violation of the Norwegian Penal Code (Straffeloven). Moreover, there must be the potential to connect the reported material to a person, address, or similar identifiers. Our conversations with police officers who interact with this system showed that those cases that were not imported were typically incomplete or unsuitable for investigation because of the following:

- Doubts about the age of the persons depicted.
- No attached files.
- The fact that the perpetrator hid behind a VPN-service and an inability to ascertain identity.

Most of these issues were related either to legal issues or technological challenges, as further elaborated in chapter 4.

2.3 Formats and sources of online CSA and CSAM

To synthesize and reduce the complexity surrounding the impact of technology on CSA, this report distinguishes between two main forms of online abuse: the sharing of inappropriate materials featuring children (often referred to as CSAM) and the establishment of direct contact and abuse of children through activities such as grooming or recorded online sexual exploitation (which represents a larger category of CSA). Behaviors related to direct contact with or the abuse of children and those related to the sharing of CSAM constitute different criminal activities, although they may use the same or similar technological channels. Therefore, in Figure 2, we distinguish between the sources of online CSAM (materials) and technological channels that offenders may use to establish contact or/and share CSAM.

In Figure 2, we group the sources of online CSAM to distinguish between the following:

- The sharing or trading of previously captured materials that preexisted online
- The direct creation of CSAM, often facilitated by mobile technology (livestreaming) and self-generated content, which enables the acquisition of material from victims (through coercing, extortion, grooming or free sharing).
- The increasing trend in digitally and artificially generated content.

The rest of this section covers these sources. Subsection 0 describes the direct creation and sharing of CSAM. Subsections 2.3.2 and 2.3.4 detail how CSAM is obtained from victims through self-generated content and live streaming, respectively. Finally, Subsection 2.3.5 describes the creation of artificial CSA imagery and videos, which is likely to become an important trend in the future.

The bottom of Figure 2 shows a classification of the various channels and platforms through which the materials are created and shared. We place different channels along a continuum going from the direct channels used for establishing contact or exploitation to the channels that are used predominantly for sharing materials (one to many or many to many channels). The framework is not meant to be exhaustive, but it rather aims to provide some clarity and synthesize the complex and largely fragmented ways in which technology has affected the creation and sharing of CSAM.

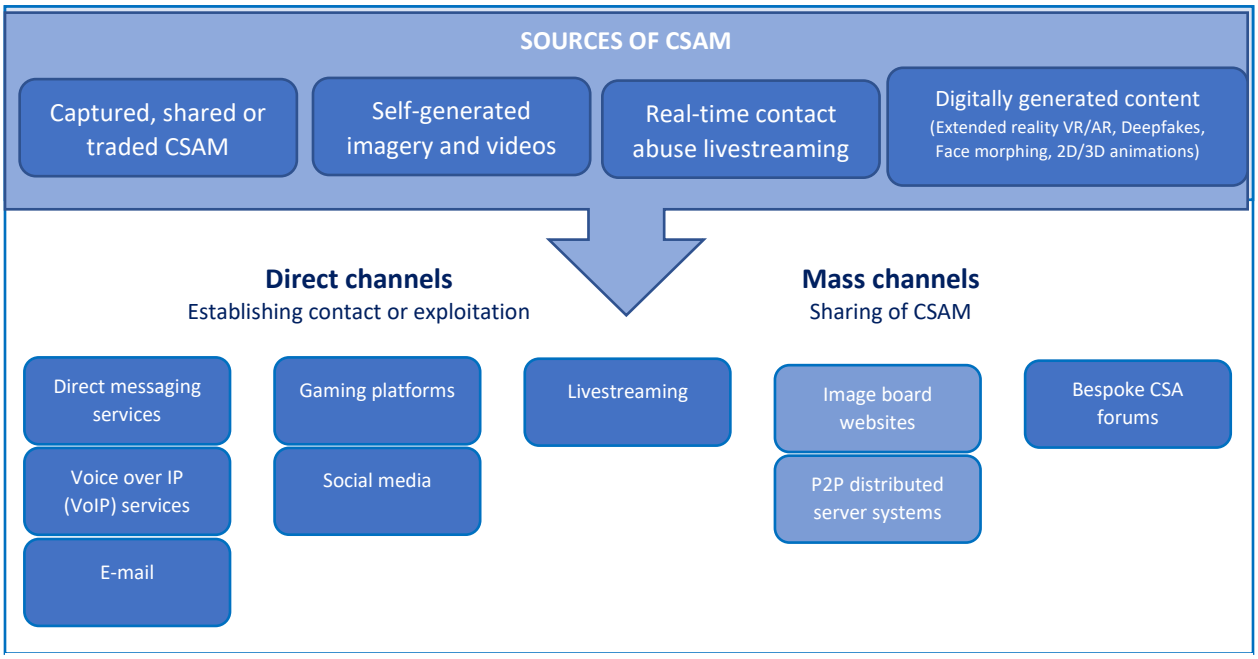


Figure 2: Formats and sources of online child sexual abuse materials.

2.3.1 Captured, shared, or traded CSAM

The majority of online CSAM includes images and videos that have been previously captured, recorded and subsequently shared with other offenders via different distribution channels and techniques (see Section 2.4). Offenders distribute and share this material among themselves through one-to-one communication methods or broad/mass distribution through one-to-many network sharing technology. This sharing of material relies on various formats, such as images, videos, live streams, or recordings ("captures") of live streams of CSA [27]. An analysis of the overall number of cases reported to the NCMEC's CyberTipline shows that out of all the sources reported as possibly containing CSAM, approximately half of them featured videos (45 million out of overall 85 million), and the other half contained images (approximately 40 million) [29]. Most reports came from internet image boards, cloud

storage and chat service providers. Since approximately 42% of images and approximately 11% of videos were identified as unique, we see that large amounts of previously generated CSAM remains in circulation (see Section 2.2).

The direct sources of online CSAM come from capturing images and videos and posting them online or facilitating livestreaming of actual abuse. The latter has become more prevalent in recent years through the widespread adoption of live streaming and Voice over IP (VoIP) technologies [28] and digital payment systems. The capturing of this material is either done covertly by offenders who record livestreams using unsecured or hacked internet-connected web cameras or through social media posts that have become indecent. Offenders can also directly solicit or coerce minors to produce self-generated CSAM content, and they can groom minors by encouraging or blackmailing them into providing videos or images.

Large archives of explicit content, among which CSAM can be found, are stored on image board websites dedicated to the uploading of images. These image boards can be hosted on:

- Bespoke illegal websites dedicated to CSAM archives.
- Seemingly legitimate websites featuring legal adult content and linked to CSAM.
- Legitimate image boards used without the permission of the owner [19].

In 2021, InHope [30] reported that 31% of all CSAM it identified was hosted on websites, approximately 26% was hosted by file hosts and 25% was hosted by image hosts. Importantly, they noted a 17% decrease in CSAM found on websites (from 48% in 2020 to 31% in 2021) and a doubling of the amount of CSAM found on file hosting websites (26% in 2021, compared to 13% in 2020) [30].

Offenders seem to use cloud storage providers as file hosting platforms to store and distribute CSAM via the passing of URLs to websites such as image boards, offender forums and chats [19]. URLs to CSAM can be further facilitated through bespoke CSA forums or sections of legitimate websites that function as forums (groups, 'rooms', etc.), which allow users to share file hosting links. A total of 81% of victims were depicted as prepubescent (aged 3-13) [19]. Particularly troublesome is the fact that the sharing of CSAM repeatedly victimizes children. Among surveyed survivors of CSA [11], whose images were distributed, 67% said that the distribution of their images impacted them strongly. In addition to the hands-on abuse they suffered, they have continued to suffer because of the permanency of the imagery and the fact that the distribution never ends.

While shared and traded CSAM represents a traditional source of CSAM, we next devote special attention to newer sources that are likely to fuel major trends in CSAM sourcing in the future: *self-generated content, livestreaming and artificially generated content.*

2.3.2 Self-generated CSAM content

Self-generated CSAM concerns sexually explicit images or videos created, transmitted, or exchanged by minors under the age of 18. These minors typically create such material themselves, using web cameras or smartphones and then share it directly with a receiver or via a growing number of platforms [31]. The

Internet Watch Foundation (IWF) reports that almost three quarters (i.e., 72%) of assessed materials in 2021 can be classified as self-generated content [32]. In just the first three months of 2021, self-generated content doubled relative to the same period in 2020. Underage girls represent a particularly vulnerable group. 99% of self-generated content features girls, and as many as 81% of all images and videos involve girls aged 11 to 13 years old in their bedrooms or another room in a home setting [32].

Self-generated content by minors surged during the COVID-19 pandemic [31], and it was identified as a particular concern by all respondents in our primary research. This trend is linked to the popularization of sexting among minors (i.e., sending sexually explicit messages to another person through electronic means) and changing social norms of online sharing. For example, a survey found that approximately 40% of children in the US believe "it is normal for people their age to share nude photos" [31]. The incidence of sending and receiving CSAM as well as engaging with self-generated sexual material among European adolescents increases as children move from early adolescence to later years [33]. This trend has also resulted in an increasing number of young people being convicted in recent years for having produced and/or distributed sexualized images or videos of people of their own age [34]. Youth from northern European countries (such as Norway and the UK) reported sending and receiving sexual material at a higher rate than their counterparts in southern European countries (such as Bulgaria, Italy, and Cyprus) [34]. For example, half of all teenagers between 13 and 18 years old in Norway have reportedly been asked to share nude photos of themselves, and 4 in 10 teenagers have admitted having obtained naked photos of others [9]. Lack of awareness about legal provisions is a common factor among convicted persons.

The problem with this source of CSAM is that not all sexting is considered illegal. Sharing of explicit content and images is legally problematic when the legal consent of children cannot be proven or when the material is further distributed without consent, used by adults above the majority age of 18 or used for cyberbullying.

2.3.3 Grooming and self-generated content

Self-generated content becomes specifically problematic when it feeds into the amount of CSAM through *child enticement,* which encompasses numerous crimes and typically involves luring children (i.e., grooming) to engage in sexual acts and other activities. The offenders communicate with children via the internet with the intent to commit a sexual offense or groom children into providing sexually explicit images of themselves. The incidence of grooming via the internet has increased by 97.5% between 2019 and 2020, as evidenced by as many as 38 million reports [35].

Groomers tend to use several techniques to solicit or deceive children into self-generating CSAM. In some cases, groomers ask children to send images or videos of themselves, and many children oblige, believing that they are in some kind of romantic relationship [14] [12]. In other cases, the perpetrator sends images of the person he or she claims to be and then convinces children to send similar images of themselves. A third method is to ask for sexualized images in return for money, cigarettes, alcohol, or other things children want.

Perpetrators pay via various digital payment options and by using money sharing services (cf. Vipps app in Norway), digital gift cards or cryptocurrency. Sometimes, the victims receive funds on an account belonging to a friend or someone who is over 18 to prevent their parents from noticing suspicious transactions from strangers [34]. Moreover, in 2019, Europol reported [9] that offenders increasingly used self-produced material to blackmail or coerce victims into creating more material and/or into including other children in the production (sextortion).

Interviewees from entertainment internet services and social media services indicated that the typical modus operandi of groomers and other offenders is to target children on gaming and social media platforms and to gain their trust before attracting and encouraging them to channels that offer streaming options and coercing them into sexual acts that are captured on camera. A recent thematic analysis of court judgments in Sweden about 50 offenders who engaged in online CSA (the median age of the offenders was 29 years old) showed that offenders typically used two main strategies to manipulate children [126]:

- The strategy most used was pressure (threats, bribes, or nagging).
- An increasingly used strategy entailed sweet-talking, using flattery, acting as a friend, or expressing love. This strategy seemed to be more often used by younger offenders.

NOVA's report on online abuse of children in Norway indicated that in 2018, 30-50% of offenders were themselves younger than 18 [36]. NOVA warns that the type of grooming by which victims feel they are part of a romantic relationship and therefore exchange photos or become sexually abused has become more common; moreover, the report mentioned that children avoid reporting these abuses [37] [43].

Civil society interviewees believe that this trend is likely to grow in the future, as interactions among youngsters and children increasingly move to digital arenas. In particular, the drivers contributing to the willing production of self-generated CSAM imagery and videos are not well known or understood. Indeed, these drivers vary, but they often include the lure of a romantic relationship, cyberbullying or the child's desire to obtain resources or recognition online.

A report in Norway indicates that romantic relationships between youth have moved to a large extent online, and young people commonly assume that "if you like me, you must share a [nude] photo with me" [37]. These new social norms "*normalize illicit behaviors and move the boundaries of what is appropriate and what is not, as children refuse the authorities' and parents' interpretation of what is normal*" (insights of an interviewee working at a child's rights organization).

Online mobbing drivers of CSAM also represent one of the greatest challenges for child protection agencies [38]. Unauthorized sharing of naked photos is the most common method of online mobbing and one of the most hurtful for victims. Kripos noted a worrying trend [39]; indeed, underage children administer so-called "exposed accounts" in which information about their peers (often from their school) is shared with other children. These accounts are administered by children, some of whom are barely 11 years old [39].

Last, a disturbing trend in the self-production of CSAM is the monetization of CSAM and sexual activities by minors themselves; in this process, minors sell explicit imagery and videos or livestream sexual acts.

Recent investigations in the UK [40] [41] and Norway [34] have highlighted cases in which minors created and sold sexually explicit content on social media platforms such as OnlyFans or through money sharing apps. The second way in which the commercialization of self-generated content occurs includes the capture of images and videos from the location in which they were originally uploaded and the further distribution of this material through online forums to receive payment for the downloads [42].

Self-generated materials harm victims in multiple ways, as materials are often shared with groups that know the victim; moreover, once posted online, the materials are difficult to track and remove. The victims seldom contact the police themselves, so the police typically obtain knowledge about the case when parents report the incident. In some cases, the victim told friends, school nurses, child protection service employees or other people outside the family [43]. The self-generation of content is likely to become one of the main challenges for the prevention of online CSAM, and it will require coordinated efforts involving schools, parents, civil society and business entities.

2.3.4 Livestreaming as a developing source of CSAM

Online CSA has become easier to access and more extreme in its process, with offenders increasingly able to target multiple children at once and orchestrate the abuse in real time [44]. Livestreaming is part of this development. Indeed, livestreaming involves the viewing of explicit content that features children or CSA in real time, which allows offenders to interact with the abusers and to request acts they want committed against the children [45]. Online streaming is likely to continue to increase [46], facilitated by an increase in the availability of Voice Over internet Protocol (VoIP) platforms, the expansion of the global reach of 4G and 5G and the widespread use of popular social media applications with embedded streaming functionalities (e.g., WhatsApp). Access to such technology has made it almost effortless for offenders to network and exploit children.

Livestreamed abuse has proliferated due to offenders' motivation to avoid leaving digital traces and incriminating materials. This proliferation has led to the practice of ordering livestreamed abuse in real time instead through the downloading of files [14]. The abuse is often organized and/or committed by facilitators who have a preexisting relationship with the children, such as a family member or a groomer [47]. Certain developing countries act as epicenters of the livestream sexual abuse trade, such as the Philippines [48] [49], where it was reported in 2020 that one in five children between 12 and 17 had been exposed to online sexual abuse [50].

Contact between offenders and facilitators is often established on websites that offer camera-to-camera sexual services for adults, which also feature CSA 'services'. In some cases, the facilitators offer so-called live shows with children; in others, the perpetrators request them. Offenders pay the facilitators through payment systems over the internet, often using digital cryptocurrency, which is harder to trace (see Subsection 4.2.2 for further discussion). The services that facilitate livestreamed abuse earn between 40-70% of the payment made by the offender [14]. Payments are always sent before the material is streamed, reflecting the financial incentive for facilitators.

Directly after the payment is received or at a scheduled time, sexual abuse is then streamed via communication services that provide chat and video. Generally, no images or videos of sexual abuse are automatically stored. Should the perpetrator or the facilitator store something and then share it on the dark web, the material becomes part of the overall volume of CSAM available online. In 2018, IWF's [51] exploration of captured live streams showed that 98% of victims were children aged 13 or under and that 28% were aged 10 or under. 18% of the abuse was categorized as rape and sexual torture, and as much as 40% of the material represented serious CSA. The most common scenario consisted in girls in their home setting, often in their bedroom or bathroom, without any adult. Offenders instruct victims to abuse themselves and to livestream the sexual abuse [51].

Victims can also be groomed by offenders to engage in online streaming of sexual activities for peers on platforms, after which the material finds its way to other online sexual offenders through 'capping'. The term 'capping' refers to the creation of permanent recordings of the livestreamed CSA via software that records the activities through a web camera. These recordings (commonly called 'captures') of livestreams are then shared on dark web forums or other bespoke channels (see Figure 2 and Subsection 2.3.1). Nevertheless, images from these captures are also produced and distributed [42]. These activities make the victim susceptible to sextortion in exchange for further imagery or illicit content. The Australian Centre to Counter Child Exploitation has reported that 'capping' is currently the most problematic trend in sexual abuse offenses and that it represents between 60-70% of the referrals made to its Victim Identification Unit [47].

Material harvested from 18 different livestreaming services, including social networks, chat sites, and mobile apps [42], shows that in some cases, children were coerced into sexual activity to gain "likes" or comments from viewers. One child, who said she was 12 years old, mentioned that she currently had 50 viewers on her broadcast stream. After repeatedly exposing herself to the webcam, she stated that she stopped the broadcast if people did not comment or "liked" the stream, as there would be "no point" in her continuing [42].

2.3.5 Digitally and artificially generated CSAM content as a worrying trend for the future

CSAM offenders generate content artificially by using artificial intelligence (AI) techniques to create new or to obfuscate existing material through animation, 3D computer generated models, or extended reality technology (virtual and augmented reality). These techniques use visual filters and image manipulation to artificially make victims appear younger and/or to obfuscate victims' and offenders' identities.

Artificially generated CSA depictions of children in virtual environments range from cartoons (2D) to hyperrealistic (3D) images and videos. These depictions have existed for a decade. One such example in 2003 was sexual 'age play' and the simulated abuse of child avatars in online virtual worlds such as Second Life. However, recent advances in technology have given offenders new possibilities for creating artificially generated CSA and obfuscating existing material.

‘Extended reality’ (XR) is an umbrella term for all types of immersive technologies, such as augmented reality (AR), mixed reality (MR) and virtual reality (VR). The form these extended realities take varies widely, but at their core they rely on simulating a three-dimensional world and presenting it to a participant in such a way that the information is processed by sensory inputs like it would be in the real physical world. XR has become popular in the adult sex industry, where it has been used to create immersive VR sexual games and films, to integrate haptic devices (teledildonics), and to extend traditional ‘camming’ in virtual chat rooms [52].

This technology is likely to be adopted by CSA offenders as it matures. For example, XR facilitates the creation of sex simulator games and/or modification of existing game characters to appear as children, which allows offenders to interact with these children as if they were in the real world. Alternatively, MR allows the augmentation of existing adult pornographic images and video into fake indecent images depicting a child by using filters such as ‘baby lenses’ that make the original participant appear more youthful.

Real children can be indirectly harmed through the legitimization and normalization of sexual interest constituting an offense [52]. Simulated sex with child avatars may involve real children as well as adults; even if it does not, it may have implications for real children by reinforcing offenders’ sexual interest in children and distorting cognitive functions about the offenses.

Altering images and creating realistic depictions that are difficult to differentiate from images of real children through Adobe Photoshop requires skills and practice. However, advances in AI have allowed individuals to automatically edit or manipulate images without the need to acquire the skills necessary to create realistic images. An example of AI-driven manipulations is ‘deepfake’ technology. Deepfake replaces the image of one person in a video with another in an almost undetectable way. Deepfake software is currently being used to create pornography that appears to feature celebrities, whereby a celebrity’s face is merged onto the body of a porn star. These technologies not only make victims appear younger but are also used to obfuscate the identity of victims and perpetrators by replacing the face of a child in an indecent image with that of another child who has never been filmed in a sexualized context. This strategy prevents the identification of victims or abusers and consequently prolongs the victims’ suffering. Similarly, new AI techniques have allowed offenders to change their voice to appear more youthful or childlike [53], which may have important implications for grooming.

In 2020, it was estimated that an AI bot operating on Telegram generated 100,000 pornographic ‘deepfakes’ of real women and girls [47]. Developments in AI have created a new category of CSAM known as “morphed” CSAM, in which a child’s face is virtually superimposed onto the body of an adult performing sexually explicit acts [54]. Such material is indistinguishable from real photos and videos. The development of AI should be of concern because it can result in the generation of new "personalized" CSAM [55].

Artificially generated CSAM material has emerged as a source of offenses and has been especially problematic because of the lack of legal penalization for this type of material [19]. In most countries, this type of crime is currently not regulated, and such computer-generated material is legally seen as protected speech [54]. Only cases in which an actual child’s photo is used are actionable under the law.

Moreover, law enforcement has struggled with the development of this technology because law enforcement officers overall lack the technical skills and tools necessary to tackle these cases. The artificial creation of content has serious implications for law enforcement, for example raising questions about the authenticity of evidence and complicating or obscuring investigations [55]. The United Nations Interregional Crime and Justice Research Institute (UNICRI), through its Centre for Artificial Intelligence and Robotics, and together with the Ministry of Interior of the United Arab Emirates, has started a global project to design a global hub and toolbox that would support law enforcement with AI tools, information and skills building opportunities and networking for sharing experiences and best practices in combatting online child sexual abuse and exploitation using AI [56].

2.4 Overview of major CSAM distribution channels

To effectively target CSAM distribution sources, it is crucial to understand how much content is shared across the diverse distribution channels that are used by offenders. E-mail was once the main method by which CSAM files were distributed. However, distribution channels have mirrored the development of new forms of online technologies [45]. Thus, CSAM distribution channels are found on websites, search engines, chat services, forum communities, social media platforms, file sharing programs, and most other places connected to the internet [18] [57] [58].

Perpetrators utilize all available channels (be they secure or not) that enable them to communicate and share CSAM on the open and dark web [14]. Even though the technology is constantly changing, most of the distribution of CSAM is made via free-to-use and public technologies [2]. Perpetrators typically choose channels based on their perceived utility and perceived risk. Peer-to-peer sharing and web browsers were the most common gateway technologies among convicted CSAM offenders in the US, and it has been shown that these distribution channels are still substantially used [24]. In recent years, law enforcement has reported that the adoption of new privacy-protecting applications has increased because of end-to-end and storage encryption and other anonymization techniques, such as the onion router (TOR) [59]. This section of the report provides an overview of the main channels used by offenders in accessing and creating CSAM. In Figure 2, we distinguish between those channels that are often used to establish one-to-one or one-to-few contacts (i.e., direct channels, such as email and messaging services) and those that are more suitable for mass sharing of CSAM (websites and image boards or distributed server systems). Naturally, a clear distinction is not possible given that these channels are often used for diverse purposes and mutually connected by CSAM users. We start the overview with the most common and traditional channels such as websites and proceed toward the channels that have appeared relatively more recently with the help of new technologies and that are likely to become more important in the future (peer-to-peer networks and dark web).

2.4.1 Web search engines and image board websites

Websites on the internet likely act as a gateway for those who are looking for CSAM, since websites and image boards contain a host of the already available (captured, shared and traded) CSAM, as seen in

Subsection 2.3.1. Web search engines are used by users searching for keywords to find access websites containing CSAM. The material might be embedded in legal pornographic websites or websites specifically catering to CSAM. Websites can also appear legitimate, but they only act as an intermediary by linking to other websites where perpetrators can access CSAM [63]. In 2021, the internet Watch Foundation (IWF) [64] identified 252,194 individual URLs (webpages) containing CSA imagery, having links to the imagery or advertising it. 39% of the children identified in the images were under the age of 11 [44].

Websites specialize in either hosting or displaying CSAM, with only 20% doing both [57]. Displaying websites seem to be focused more on organizing material (e.g., folders formatted by year or month for easy access and promotion) than on hiding it [57]. Research conducted on CSAM websites has demonstrated that most websites do very little to hide their users' intentions [65]. The primary aim of websites displaying CSAM is to garner viewers and distribute the media. CSAM websites with much content and connections to other CSAMs are more likely to last [57]. Therefore, they make few attempts, visually, to disguise their users' intention [65]. Over 27% of websites displayed CSAM content in their home directory [57]. Many websites are freely accessible and do not require people to register to view content. Websites often contain a combination of blog-based and generic website-based content. It is common for multiple display websites to obtain the CSAM they feature from the same hosting website or hosting hubs/boards [57].

Most of the imagery is stored on an image hosting website (also sometimes referred to as an image board). Image hosts allow users to upload still images that are assigned a unique URL and can be embedded to display on third-party websites, such as forums or social networking sites. This technique is commonly employed to distribute CSA images [42]. By using image hosts, distributors of CSAM imagery exploit legal loopholes that exist in various countries to ensure that their website remains online and immune to takedown.

Understanding the dynamics of these online communities is one way to support the detection of illegal content. Hosting CSAM is riskier for websites than displaying it. Therefore, people behind hosting websites unsurprisingly go to greater lengths to mask/hide their content. For example, folder and files are not explicitly titled, as hosting websites avoid the use of explicit keywords to describe their content. Comparatively, people behind displaying websites less often attempt to falsely label their CSAM folders using explicit keywords. People on hosting websites have likely used alphanumeric or disguised folder and file names to conceal material, while people on displaying websites have been more explicit. Search engine providers, such as Google and Microsoft's Bing, play a critical role in identifying and removing CSAM-related URLs from their search engines (e.g., in 2021, Google reported to have reported and removed 1.18 million URLs containing CSAM from the Search index through their proprietary automated software and human reviewing) [128]. More on these efforts can be found in Section 3.5.

2.4.2 Social media applications and instant messaging services

The rising popularity of social media applications and their widespread use among children and youth makes these media attractive both for approaching or grooming children and for sharing CSAM [44] (see

Subsection 2.3.2). Because they make it easy to access a large number of children and simple to create multiple accounts, social media and gaming platforms are used by perpetrators to groom children, initiate sexual relationships with minors, and/or communicate and access information about their victims [66]. There are also instances where fake social media accounts are created to spread private pictures and videos of underage victims as well as their personal information [44].

A survey of Norwegian children in 2021 showed that they access porn and other inappropriate material largely through image and video sharing platforms such as Instagram and YouTube or through social media platforms such as Facebook and Twitter [71]. Moreover, TikTok, widely used among Norwegian children aged between 9 and 10, is a popular place for the sale of homemade pornography [71]. Minors can allegedly privately post on TikTok explicit videos through the "Only Me" feed [72], and this content can then be accessed by anyone with a shared password.

Social media companies' instant messaging systems that use Voice over internet Protocol (VoIP) and end-to-end encryption particularly facilitate CSA and the sharing of CSAM. CSAM is regularly found and removed by diligent social media platforms. Facebook [26] in particular reported that in the second quarter of 2022, 20.4 million content actions (such as sexual exploitation) were deemed to endanger children, representing a significant increase from 16.5 million content actions in the first quarter of 2022. Similarly, in the period between January to March 2022, TikTok removed 102 million problematic videos. Grounds for removal include violations of minors' safety (41.7% of removed materials) and adult nudity and sexual activities (11.3%). Comparatively, the same category of nudity accounted for 21.3% in the period between July and September if 2020 [73]. TikTok claims that the removed videos represent approximately 1% of all videos uploaded to TikTok [73]. The biggest providers of instant messaging services, such as Facebook's Messenger, Google's Messages, What's Up, Skype, Twitter, etc.) currently report the largest share of CSAM material to clearinghouses (e.g., Meta contributes 93.4% of all reports that the NCMEC receives, Google approximately 2.5% and other large providers such as Snapchat, Microsoft, Twitter, TikTok and Imgur jointly contribute approximately 1.5% of those reports) [25].

However, the significant move toward end-to-end encryption by social media ESPs exacerbates the difficulty of following and detecting CSAM and online CSA because these encryptions reduce the ability of both ESPs and law enforcement to monitor communication. The instant messaging application WhatsApp has reportedly been used to create chat rooms specifically for CSAM distribution [67]. Applications employing end-to-end encryption cannot detect CSAM shared in private messages unless users report it directly. Nevertheless, WhatsApp indicates a banning of 300,000 accounts per month because their users share CSAM through user reports; the application detects the unencrypted information in users' profiles and group photos [68].

An independent investigation of groups based on pornography on WhatsApp and Telegram instant messaging applications over a period of one month (June/July 2020) identified 1,299 pornography-based groups on WhatsApp [69]. None of the groups were removed after they were actively reported, and only four of the 29 reported users were banned. Out of 350 adult pornography channels identified on Telegram, 283 were studied in depth, and 171 channels were removed after they were reported through multiple channels [69] [70]. A further discussion about the challenges emerging in the private–public cooperation for the prevention of CSA and CSAM sharing can be found in Section 4.2.

2.4.3 Peer-to-peer networks

Peer-to-peer (P2P) networks are a common form of file sharing for acquiring music, movies, and other digital materials. In its simplest form, a P2P network is created when two or more computers (peers) are connected and share resources without going through a server. The usual way to obtain access to a global P2P network is with the use of special network protocols and applications by which a direct connection is set up among users over the internet. The applications used to join a P2P network are available, user-friendly, and free.

Typically, users request files using search keywords and receive information about the files, such as its name, size, and network location. Users can then select and download the desired files, creating new copies on their local hard drive that are also shared with other peers in the network. Closed P2P file sharing networks mostly work in the same way, but users need an invitation to join the network [14].

P2P networks are part of the most frequent technologies used by offenders to share CSAM with each other [24] [60]. Moreover, these networks likely contain the largest share of online CSAM [45]. Because of its widespread use, P2P software is often a gateway technology to access and share CSAM for the first time [24]. Using P2P networks as distribution channels is particularly attractive because they do not require servers and can, therefore, transmit CSAM while avoiding oversight from service providers [27]. These networks make it possibly for a small group of offenders to supply large amounts of CSAM [60]. An investigation [61] of the P2P network eDonkey2000 revealed that 0.25% of all entered queries were related to pedophilia. Since the identification method in this study was based on a predefined list of keywords and new or previously unknown terms could not be detected, the actual proportion of CSAM-related queries in this P2P network is likely to be higher. The Kripos investigative team identified the following P2P file sharing networks as prominent in the sharing of CSAM in Norway: BitTorrent, Gnutella and eDonkey2000 [62]. Interviewees from Norwegian law enforcement and Kripos confirmed the prevalence of this trend in Norway:

> "*P2P are the largest channels for CSAM sharing that we meet in our cases. We also meet social media channels and other direct messaging applications (Skype, WhatsApp). In cases we meet children and minors who do not understand what they are sharing or doing but also adults who share [CSAM] with each other.*"

To avoid detection, P2P communities increasingly need to select peers and strictly control access, e.g., with affiliation rules, codes of conduct, division of tasks and strict hierarchies, to enforce rules and promote users within the network. To mask the country of residence, perpetrators use open proxy servers or virtual private network (VPN) solutions offering connections in Norway.

VPN technology is used to create secure and encrypted connections ("tunnels") between individual computer devices and a VPN service. When this technology is used, the police can only see that the person is using a VPN service, which disguises the IP address of the that person. The VPN service changes the IP address of individuals and makes it appear as if it originates from the country in which the VPN server is located, whereas the individual is based in another country. Perpetrators take advantage of this technology to disguise where they are. Law enforcement depends on VPN service

providers to obtain logged user information. However, the lack of regulations governing VPN providers has obstructed this process [14].

2.4.4 The dark web and distributed server systems

The ‘dark web’ is a term that refers collectively to all communication networks that are covert. These networks are not indexed by search engines and are accessible only via authorization or through specific software [74]. For offenders, the dark web provides a more secure and anonymous platform for CSAM distribution. These properties make it difficult to estimate the full extent of the illicit traffic going through the dark web [75].

The dark web is most frequently reached using the Tor (The Onion Router) network. Despite the existence of other dark web software, the Tor network remains one of the most frequently used and well-known and is favored by users who wish to hide their activities [76]. Users access the Tor network using the specialized ‘Tor Browser’. The latter works by routing traffic through other users who have declared themselves to be nodes within the network. Whenever a Tor user, referred to as a source, joins the network through Tor Browser, a virtual circuit is constructed using a random selection of (usually three) intermediate Tor nodes located around the world. This virtual circuit is used for approximately ten minutes, after which a new virtual circuit is created. This circuit contains three types of nodes: (1) entry nodes—the first node in the circuit that accepts incoming traffic; (2) intermediate nodes—which transmit data from one node to the next; and (3) exit nodes—the last node in the circuit that delivers traffic to the internet.

When a Tor user requests access to a website, the request is encrypted through multiple layers and sent to the entry node. From the entry node, the request is transmitted to an intermediate node in the virtual circuit. After each hop in the circuit, a single layer of encryption is taken off from the request before passing it to the next node. Once the request reaches the exit node, all the encrypted layers are removed, and the unencrypted request is sent to the web server on the public internet. In this process, any information about the source is lost, and the Tor user remains anonymous. Traffic can only be traced back to the previous link in the virtual circuit. An analysis [77] of the type and popularity of the content on the Tor network over a period of six months in 2015 concluded that the majority of these websites were criminally oriented. While only 2% of websites hosted CSAM, they attracted as much as 80% of all requests for access.

The term ‘hidden services’ often applies to settings with covert networks. It is known that perpetrators misuse Tor’s hidden services to host forums dedicated to CSAM [78]. An investigation has suggested that from 2019 to 2020, the use of hidden services to distribute CSAM increased by 155% [79]. In 2019, there were 3.45 million accounts registered globally across the ten largest CSA dark websites, a near 20% increase over that of the preceding year [80]. Europol’s investigation in Germany in May 2021 uncovered a dark website focusing on CSAM with more than 400,000 registered users [75].

Tor's end-to-end encryption provides a built-in countermeasure that provides anonymity to distributors and consumers of CSAM [2] while decreasing the risk of being detected. Both VPN networks and the dark web can be used for this purpose. VPNs hide the source IP addresses by directing web traffic

through a VPN intermediary, while Tor sends traffic through a series of relays that prevent identification of the source IP addresses. Much of the sharing of CSAM on the dark web takes place in the form of sharing links to files found on the open internet. Partly due to the limited storage and bandwidth capacity of the dark web, most of the available sexual abuse material is found on platforms on the open internet, in cloud-based file storage services and file sharing networks [14].

More extreme and newer CSAM are found on the dark web [81], but frequently the link to that material points to locations where this material is stored on the internet. Offenders are often encouraged through open web forums, sometimes actively, to move to sites on the dark web.

2.4.5 Forums

Perpetrators can communicate with like-minded people through chats and forums found on both the dark and open web. Chats that sexualize children are covered by the Norwegian Penal Code section 311 [14]. The services used for these chats are most commonly end-to-end encrypted. Moreover, perpetrators tend to use pseudo or hidden identities, which enable them to freely share not only thoughts and fantasies but also experiences of actual physical sexual abuse of children. Some of the forums make it possible to exchange files, resulting in chats going on while the sexual abuse material is being shared.

A collective approach to improving operational security for the users of forums has emerged [44]. In the UK, forum users regularly publish information and safety manuals aimed at avoiding detection by law enforcement authorities [44]. To evade law enforcement operations, forum communities select participants and strictly control where meetings take place; for example, these communities implement rules of affiliation, codes of conduct, division of tasks and strict hierarchies, and enforce rules that promote users based on their contributions (the recoding and posting of their abuse of children) to the community.

An analysis of the topics discussed in CSAM-dedicated dark web forums performed by Crisp [47], an online safety technology provider, showed that two-thirds of the discussion topics benefited from ‘tradecraft’ and tools that may facilitate access and abuse. As much as one-third of the discussions were devoted to providing advice on platforms on which offenders seek to engage children or vulnerable users, as illustrated in Figure 3. “Tradecraft” topics often feature an exchange of information about security measures to conceal criminal activities, such as encryption and anonymization services and deletion (wiping) software.

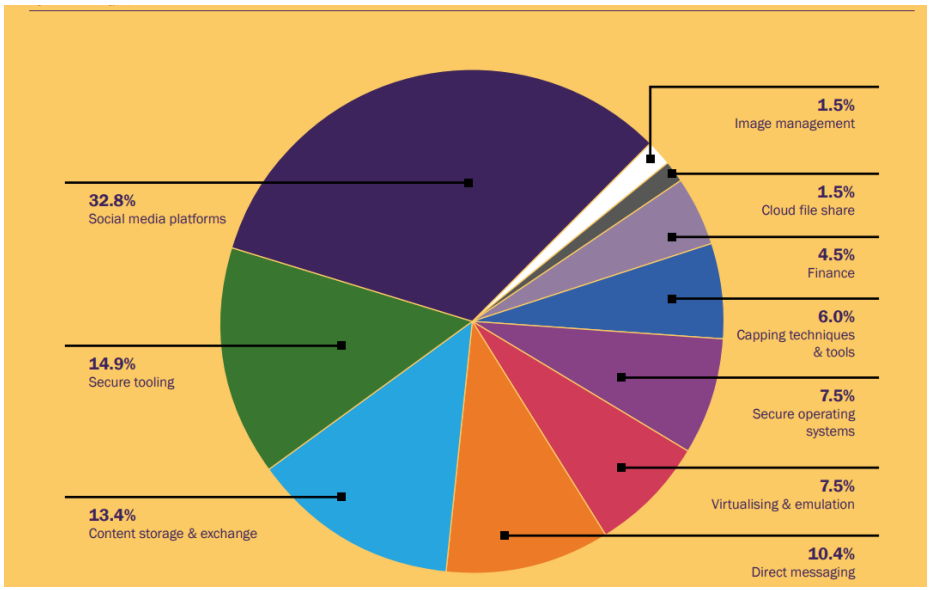


Figure 3: Topics most frequently discussed by offenders on the dark web forums. Source: We Protect Global Alliance (2021). Global Threat Assessment 2021 [47]. Page 28.

Forums are also often at the center of this exchange of information via other channels. For example, an investigation by IWF found that in the case of livestreamed CSA, as much as 73% of identified content was embedded into 16 forums dedicated to the distribution of captures of livestreamed CSA [51]. Image previews of livestreamed CSA videos have been used to advertise for paid downloads of the full video capture from third-party cyberlocker websites. Cyberlockers pay the uploaders of content for each sign-up and subsequent download of their files. The use of paid cyberlocker accounts, therefore, not only prevents the removal of captures but also enables offenders to make a direct financial profit from the distribution of the material.

Chapter 3: Law enforcement's countermeasures and techniques for the detection and prevention of CSA

The previous chapter elaborated on the ways in which perpetrators use technology to contact and groom children, to coerce children to create sexual images and videos, and/or to record their sexual abuse of children. Significant progress has been made by law enforcement in terms of tackling online child sexual exploitation and abuse in a relatively short period of time [5]. For example, law enforcement agencies continuously monitor P2P network communication to identify major CSAM distributors, to locate and prosecute persons in possession of CSAM, to identify child victims and to remove material [82].

A few years ago, in the period between 2000 and 2011, most apprehended CSA offenders did not employ strong technological countermeasures to disguise their identity [83]. For example, 54% of Australians arrested for CSAM possession did not make any effort at concealing who they were [84]. The rationale behind this behavior may have relied on the low technical knowledge and expertise of the perpetrators in setting up a secure environment. While offenders have continued to adapt to changes in internet-related technology, that adjustment has not always been rapid. The majority of known CSAM is not hosted on the dark web but on easily accessible websites on the internet [2]. Indeed, the majority of CSAM domains utilize free-to-use and public websites.

However, CSA perpetrators have gained technological skills and increasingly used technology to get better organized and use forums and other forms of communication to share information about how to improve their security and anonymity [4]. To protect their anonymity, offenders also now use protected network connections (virtual private networks), encryption and proxy servers; they also access the dark net to communicate [83].

This development has forced law enforcement to acquire knowledge and tools and to develop more sophisticated methods to better detect and prevent CSA. This chapter provides an overview of the main technological advancements in the improvement of countermeasures in the fight against online CSA.

3.1 Hash database and hash list matching

Hash databases or hash lists represent the main means of identifying CSAM perpetrators globally. Hash functions are algorithms that create short fixed-length numerical values (so-called hash values) from a potentially unlimited input length. The hash algorithms are constructed in such a way that the same input data always generate the same output data. The hash value can, therefore, serve as a digital fingerprint to uniquely identify the underlying material. The two most well-known hash functions are Message-Digest Algorithm 5 (MD5) and Secure Hash Algorithm (SHA) [27], [85].

Hashing is one of the primary technologies used by law enforcement, social media platforms and other private companies to detect known CSAM [27] [86]. In a hash-based detection mechanism, confirmed CSAMs (typically images) are saved with a unique hash value in a database or a hash list. Law

enforcement and ESPs can use this database to compare the hash of uploaded material for matching image hashes to automatically find known CSAM faster without the need for analysts to view the same images repeatedly [1]. Thus, scanning material that users upload online for matches in the hash lists effectively prevents known CSAM from being uploaded, and/or it flags illegal content to identify distributors of CSAM and prevent revictimization.

By analyzing the digital, visual and audio content of images and videos identified through hash databases, victim identification experts can retrieve clues, identify overlap in cases and combine their efforts to locate victims of CSA [87]. The IWF and the NCMEC maintain the two largest hash databases. The NCMEC added 1.4 million hash values to their growing database of over 5 million hash values in 2021 [6]. Interpol's International Child Sexual Exploitation image and video database holds 2.7 million identified images of abuse (hashes), which have led to the identification of 13,794 offenders [87].

The main hash matching solutions that industry and law enforcement employ are Microsoft's PhotoDNA and Google's Content Safety API and CSAI Match (for videos). PhotoDNA is an image identification software that creates a hash (unique digital signature) of an image that is then compared against signatures (hashes) of other photos to find copies of the same image. These solutions are provided freely to NGOs and eligible businesses. Google reports to have contributed (cumulatively over years) 1,997,505 hashes to the NCMEC database through their proprietary tools that have identified confirmed CSAM materials on their platforms [128]. Examples of major ESPs using hash-based solutions from PhotoDNA or Google (or both) are Meta (Facebook), Snap Inc, Twitter, Dropbox, etc. However, smaller service providers and those without access to hash value databases (nonmembers of IWF or NCMEC) are limited in their ability to detect CSAM [57]. The lack of skills and resources for smaller service providers makes the issue particularly daunting. Only around 70 companies were using the PhotoDNA solutions in 2022 [88], illustrating the limitations in the scanning of uploaded material globally.

Hash-based detection mechanisms have some well-known limitations [86]:

- They have lower ability to detect new and unidentified material.
- They show weaknesses in identifying (original) materials that have been modified through transcoding, scaling, resizing or color adjustments.
- Other formats, such as video, need to be integrated into searches for CSAM.

Due to these limitations, hash databases must be regularly updated with hash values of new and modified CSAM to increase the possibility of finding reuploaded material. There exist many hash and URL lists, but most of them are not linked, suggesting that much of the work done across organizations occurs in silos and that there are duplicated efforts [4]. Downloading and using hash lists require a substantial amount of investment in terms of technical capabilities and time commitment. However, a lack of guidance or mandate from governmental agencies about how hash lists should be implemented has hindered efforts because there is a need for databases to be linked to ensure that images are shared appropriately between agencies and across sectors, nationally and internationally.

It is important not to reply too much on hash lists, as offenders may learn to circumnavigate them to avoid detection (e.g., by changing the pixels). Hash algorithms, such as PhotoDNA, have made

improvements in resisting some alterations in images, which has enabled them to detect modified copies of the same image. These improvements have included the resizing and minor color alterations of images [45]. However, a major limitation is the inability of these algorithms to detect new CSAMs. This is particularly worrisome given that self-generated content proliferates and that as much as 82% of the total number of processed URLs by the IWF in 2021 was yet unknown. Nevertheless, it is not possible to fully discern whether this volume truly represents newly produced content that is in circulation and that has still not been identified by law enforcement, or if this content has not been included (identified) by the IWF searches. In this respect, the coordination and sharing of information between law enforcement agencies and child protection institution is crucial.

3.2 Web crawlers

The websites that host and display CSAM are often linked [63]. Web crawlers assist law enforcement in detecting CSAM and mapping relationships between these websites. Web crawlers are automated scripts or programs that are used to move across many websites to browse and collect data about each visited website based on predefined criteria. These criteria are specific characteristics of CSAM websites, such as keywords commonly used by offenders and hash values of known CSAM. A list of websites that have already been identified as containing CSAM is the starting point of a crawl. The web crawler exploits the connectiveness between websites to find new webpages by following the hyperlinks on each webpage visited.

Web crawling technology works much faster than manual methods of CSAM detection [45] for identifying the volume of known CSAM on the internet [86]. Offenders are aware that large popular websites allow law enforcement to crawl them, which in turn makes it more difficult for offenders to access certain websites linked to large websites. The Canadian Center for Child Protection (C3P) has built the web crawler *Project Arachnid* [89], which uses Microsoft's PhotoDNA technology and hash databases from several organizations: the NCMEC, the Royal Canadian Mounted Police and Interpol. Once the crawler has identified some material as CSAM, the material is pushed to a classification system and three different analysts to verify the underlying content. When the material is verified, these analysts send a notice to the hosting provider to remove the material and follow up that the hosting provider deletes the content. Over a six-week period, Project Arachnid processed over 230 million webpages. Over 5.1 million of them hosted known CSAM, with over 40,000 unique images [45]. These numbers highlight the utility of web crawlers for CSAM detection. To take down the material, web crawlers are also used to search the dark web, but because hosting providers are not known, web crawlers can only identify links from dark web websites leading back to the internet.

The IWF uses a web crawler with PhotoDNA that visits several million webpages per day searching for CSAM. The objective of the crawler is to protect victims from revictimization through material being distributed across the internet [85] [90]. The IWF also automates the review process by incorporating AI classifiers to increase the likelihood of the crawled material being CSAM. Most of the material that is found today is usually old and has already been widely distributed (see Subsection 2.3.1).

The main limitation of web crawlers is that web crawlers successfully identify CSAM websites only if appropriate criteria (e.g., keywords and hash values) are selected. Law enforcement staff not only must possess the necessary skills to operate web crawlers but also must select criteria and find major websites. Selecting appropriate keywords and hash values requires prior research, and these values must be continuously maintained afterward as the field evolves. For example, keywords must be effectively chosen to avoid false positives from websites that contain legal, adult pornography [91]. Therefore, it is important to gain an understanding of how offenders label files or words used by people who are seeking CSAM. Law enforcement is also required to regularly check the crawler's results [45].

3.3 Website fingerprinting

Offenders can easily access CSAM websites on the internet through their web browser, which is the simplest way of accessing CSAM and the primary gateway for people who are looking for CSAM for the first time. In this scenario, the offender obtains access to the CSAM website by visiting a domain name ("example.com", the second-level name "example" belongs to the top-level domain [TLD] "com"). There is at least one IP address associated with the domain. The IP address represents the server's location on the internet where the material is kept, and people are sent there when they visit the domain.

Web search engines and internet service providers (ISPs) have a list of domains and keywords preventing offenders from accidentally and purposefully accessing CSAM websites. In employing countermeasures, scanning for displaying websites is easier, as these are more likely to display material prominently and use descriptive, accurate names for their files; they are also more likely to strategically target hosts, which can have a greater impact on the distribution network [92] [93]. The reason is that the CSAM that is present on hosting websites can be disseminated by numerous display websites. When a hosting website is removed, CSAM is effectively removed from all displaying websites.

Administrators of CSAM websites consider the server location and domain name part of their "burner website". A burner is an inexpensive website that is designed for temporary use; after a certain amount of time, that website may be discarded, which means it can be shut down as a results of efforts by law enforcement agencies, internet service providers (ISPs) and domain name registrars. Therefore, offenders focus their efforts on strategies to swiftly move their operational environment to new hosting locations on the internet. They employ some strategies to stay online [84]:

- *TLD hopping* occurs when a website retains its second-level domain name but changes its TLD. For example, owners of "badsite.no" also register domains such as "badsite.se", "badsite.com", "badsite.info" and other similar names. Changing the TLD allows a website to remain online after the original domain has been taken down; hence, the website remains recognizable and easy to find [94].
- *Domain tasting* constitutes a practice that exploits the add-grace period to gain access to a domain at no cost [84] [95]. An add-grace period refers to the number of days during which a domain name registration may be cancelled at no cost. It was originally introduced to allow people registering a domain name to correct typos or other errors [96]. *Domain kiting* is an

extension of domain tasting. It is the practice of repeatedly registering and deleting a domain name with one registrar because this registrar does not check for reregistrations of the same domain.

On CSAM websites, people typically do little to hide their intentions [65], and there is no need for these websites to move the webpages to a new host. It is likely that rehosted websites will look the same, which creates an opportunity to automatically detect the resurfacing of CSAM websites based on comparison techniques that detect visual similarity. When websites repeatedly change hosting providers [89], there is an opportunity to automatically detect their resurfacing.

Websites can be compared along many extracted features; these features include texts and pixel-based features that underline website structures, style sheets and network traffic patterns. The use of multiple textual and structural features in combination with the analysis of visual similarities tends to be more successful. Methods detecting visual similarity focus on the graphical content of a site, for example by looking for matching images and, in particular, for recurring image components such as logos. A multiheuristic approach is preferred because it considers block level similarity, text similarity, image similarity, etc. The addition of image classification and CSAM detection acts as a further verification method and prioritization measure. The wording of peripheral website features (such as disclaimers, copyright notices or legal and pseudolegal assertions) can often be recycled unchanged. The grammatical and orthographic errors can act as signatures for secondary content that is transferred from one site to another. Content features can be used to identify suspicious sites, such as specific HTML comment text and identifiers included in traffic monitoring and ad placement scripts [97] [98].

Nevertheless, techniques measuring the visual similarity of content may produce false positive matches, given that the HTML structure is often repeated across websites that use the same templating system (or website generation kit).

3.4 Filename and metadata

One challenge when distinguishing between regular pornographic and CSAM files is that the latter use very similar sex-related vocabulary and terms. Researchers have approached this problem by building statistical machine learning models to analyze features from files and their metadata to create a distinction between these file types. A machine learning model can recognize queries of perpetrators or filenames in the data of P2P networks that contain CSAM with a recall rate of 0.78 [99]. Models include classifiers to distinguish filenames from titles of pornographic webpages relative to Wikipedia articles [100].

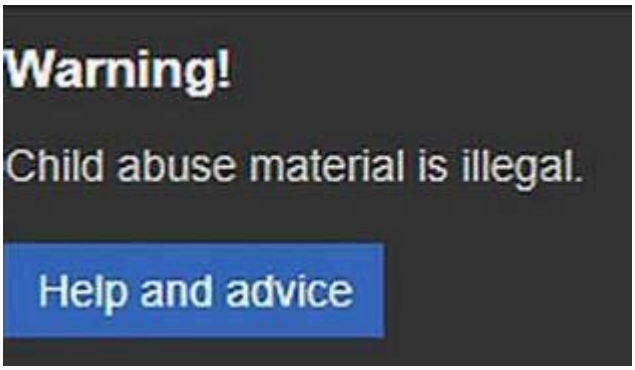
3.5 Pop-up warning messages and internet rerouting

Pop-up warning messages and rerouting are used to prevent offenders, particularly first-time offenders, from accessing CSAM. Search engines, such as Google and Bing, present warning messages when individuals type CSAM-related search terms into the search engine. Pop-up warning messages reduce a

potential offender's perceived sense of anonymity, increasing the perceived risks of getting caught [101]. Warning messages (particularly those containing information about the activity being illegal) effectively discourage individuals from accessing a "honeypot" (pretend) website claiming to contain legal pornography (relative to 60% of individuals who attempt to use such a site without warning, only 38% of individuals did so after being shown the warning message [101]).

Internet rerouting is a technical solution that routes away data traffic from domains that the police identified as containing CSA to a service provider "stop site" or a police-owned “stop site” (this technique has been used in Norway since 2004). The stop site states that the user's web browser has tried to access a website used for distribution of sexual abuse material and refers to the applicable penal provisions. It also states that the stop site is intended for preventive purposes and that no user information is stored. Similar efforts to block searches by Google and Bing found a 67% reduction in web searches for CSAM on those search engines in a one-year period (between 2013 and 2014) [21]. Comparing the effect with the Yandex search engine in Russia, which did not implement the same blocking efforts and has not seen a commensurate drop during that same period, indicates potential positive causal effects of site blocking efforts [21]. However, because Google and Bing are simultaneously used for both blocking and providing warning messages, it is not possible to distinguish the effectiveness of the blocking and that of warning messages and whether they constitute deterrents. We could not identify any newer study for which a comparison had been performed.

Warning messages and rerouting techniques do not per se offer support or assistance for the offenders, but in many instances (e.g., on Google or Bing warning messages), a link to a helpline is provided, as seen in Figure 4a. In addition to these deterrence measures on the internet, similar prevention techniques have been implemented in open P2P file sharing, as explained in the next section.



a) Bing search engine’s warning message.

b) Police2Peer warning message in P2P networks.

Figure 4: Examples of pop-up warning messages on search engines and on P2P networks.

3.6 Monitoring peer-to-peer networks

The monitoring of P2P network communication assists law enforcement in identifying major CSAM distributors, locating and prosecuting persons in possession of CSAM, identifying child victims, and removing CSAM sites [82]. P2P network monitoring involves law enforcement using tools to collect data about users who attempt to download CSAM. Included in the data captured are the IP addresses, hash values and file names existing on those computers that are part of the communication. One such example of a P2P network is Police2Peer [102], a project that entails technical prevention under the direction of Europol and the European Multidisciplinary Platform Against Criminal Threats (EMPACT) and is directed at users of open P2P file sharing networks. On those networks, files are created and their names indicate that they contain CSAM; however, these files do not contain anything or contain images or videos of police officers explaining the risks associated with the distribution of such material. This content raises people's sense of the risk of being detected and motivates peers to cease distributing CSAM (see Figure 4b).

A study evaluated how effective a P2P network (Gnutella) was in stopping the top 1% contributing computers and suggested that law enforcement could reduce availability of CSAM on that network by 30% [103]. P2P network monitoring also has the added effect of alerting perpetrators about the active law enforcement presence on the network, which may influence some CSAM consumers' decisions about whether to continue viewing the content.

However, this strategy is limited in several ways. Indeed, it requires intensive labor and investment of law enforcement resources [103], which is amplified by the mere quantity of CSAM and the need for technological skills. Since the method relies on hash list matching, new images that have not been previously identified by hash values may go undetected by law enforcement (see Section 3.1). The IP addresses can also be changed at the will of the offender. Law enforcement must use relevant software for forensic analysis, conduct proactive investigations and serve subpoenas on internet service providers to identify the accounts to which an IP address has been allocated. Further inquiries are required to identify possible individuals linked to these addresses before seeking and then executing search warrants.

In Norway, Kripos and a dedicated team by the Trøndelag police district, Seksuelle Overgrep mot Barn over Internett (SOBI), has monitored selected P2P file sharing networks to identify computers that download, provide access to and distribute files classified as CSAM. This tool linked approximately 15,000 unique Norwegian IP addresses to sexual abuse material distribution between 2017 and 2018. Further investigation is required to verify whether the users of these IP addresses have accessed CSAM. As several users can operate from one single IP address and one user can have multiple IP addresses over the course of a year, the number of IP addresses cannot fully reveal the number of people who access CSAM files.

3.7 Automated detection techniques using machine learning and artificial intelligence

The abundance of CSAM on the internet has necessitated the use of automated analysis techniques for faster detection. Detection techniques have traditionally relied on keyword analysis and hash value matching. The limitations of these two methods have led to the development of tools that integrate machine learning techniques for the purpose of automatic detection of known illegal imagery and for the identification of new (yet unconfirmed) CSAM.

The development of machine learning algorithms and artificial neural networks has substantially improved the ability to classify CSAM materials from other adult pornographic material and respond to attempts to circumvent hash detection. Deep learning methods that analyze facial cues are more robust and invariant against modifications relative to the use of hashes and filenames [104]. Unique facial characteristics (e.g., the distance between the eyes, nose width, etc.) are used to generate a distinct identifier for each individual, which can be evaluated against a facial recognition database to find any instances of the suspect (or victim).

Feature extraction of a set of facial features and body's skin tone have been used to design a classification system that can distinguish between CSA content and non-CSA content, as well as assess the age of individuals with 74.19% accuracy [105]. The main challenge in the classification of CSAM is the presence of legal, adult pornographic material [45], as well as the presence of not-illegal material of children. It is particularly difficult to effect the classification by age in the case of postpubescent children (i.e., aged between 15 and 16), and these classifiers show low accuracy rates [106]. In the classification of videos, adding audio information significantly improves the accuracy of CSAM detection.

The multimodal classification approach used to identify CSAM videos and images has yielded greater discrimination, improving the accuracy of CSAM detection. Using a single form of detection (e.g., skin tone analysis) is not reliable in differentiating CSAM from adult pornography. Thus, the use of multiple methods to classify material and detect CSAM constitutes a more robust and accurate approach [27] [104]. CSAM detection methods [107] that use multiple features to identify CSAM (e.g., shape, text, and color) perform better than those that use a single feature (e.g., skin color).

One of the main challenges for further development is the lack of real CSAM datasets that could be used to test algorithms due to the fact that information is the property of the industry; there is also a lack of uniform international standards in the labeling of CSAM and disparities in legislative frameworks across the world, which we further discuss in Chapter 4:. Thus, researchers need to work with law enforcement to gain access to databases of existing CSAM to deliver better algorithms to be used in detection. To date, very scarce research exists on the detection of CSA in livestreaming formats due to difficulties in capturing encrypted information flows that these systems often use. It is especially difficult to find livestreaming of CSAM, as this content leaves very little to no digital trace after the broadcast is over, unless it has been recorded. Future research on this topic can aid in recognizing ways to harmonize methods across different legislations.

As indicated in Subsection 2.3.5, artificially generated CSAM has become more prominent, posing a particular threat to law enforcement's deterrence efforts due to the lack of legal provisions and the

inability to penalize deepfake manipulated CSAM that can be artificially generated through the manipulation of actual images. The rise of deepfakes is concerning because the media these deepfakes produce is indistinguishable from real photos and videos. However, automated methods have also been used as countermeasures. Automated tools exist to support police in preventing CSA in online chat rooms [108]; these tools make predictions about the age and gender of the individuals standing behind online aliases and who are engaged in sexualized conversations with children and assist the police in identifying former CSA offenders who resume criminal activity online. For example, "Sweetie" was a computer-generated, virtual child used to expose online sexual predators. Sweetie is programmed to not only look like a ten-year-old girl but also to use tone, facial expressions, and movements to replicate those of a real child, which allows for the obtention of identifiable information about sexual predators [109].

Artificially generated CSAM contents represent a particular concern for the criminal investigators who were interviewed in Norway:

> "*We begin to see deepfakes in which children's faces are pasted on a small adult's (porn star) body. This is likely a trend that will increase in the future. Virtual reality is likely to further emerge as an arena for abuse. The porn industry is moving in the direction of selling sex toys that simulate acts in videos. This [technology] will become the next big problem area. What we believe will increasingly happen is the live streaming of abuse in other countries."*

Chapter 4: Structural and legal challenges in combatting CSA online

Previous chapters highlighted that the prevention of online CSA is a complex, multifaceted phenomenon that cannot be undertaken or regulated by one entity only. Each of the multiple stakeholders (civil society, parents, educators, law enforcement, firms and regulators) can only partly impact the issue and therefore must rely on cooperation. Educators and parental efforts have been successful in raising the awareness about online dangers, but social drivers of sexualized image sharing, the normalization of online porn access and the increased sophistication of groomers impose severe challenges on the deterrence efforts that rely on civil society [110] [111] (see the discussion in Section 2.2). On the other hand, law enforcement's ability to effectively tackle cases online depends on the legal aspects and provisions that specify what the diverse stakeholders' responsibilities are in the detection and prevention of online abuse; this ability also depends on collaboration with electronic service providers (ESPs), which can act both as facilitators and gatekeepers in the prevention and detection of CSA crimes on online platforms.

Our analysis of the academic literature and the interviews we conducted with diverse stakeholders indicates two major challenges for the future: legal challenges and challenges emerging out of the cooperation among diverse stakeholders.

4.1 Legal frameworks and lack of standardization as obstacles to online CSA detection

4.1.1 Legal ambiguities and lack of global enforcement of regulations

Regulations, rules and compliance guidelines on the responsibilities of diverse stakeholders in preventing CSA online differ significantly across countries. A recent UNICEF survey [5] across 29 countries revealed that as much as 86% of countries have only partial domestic regulation in place for detecting, reporting and taking down child sexual abuse material online. These countries have reported a lack of dedicated law enforcement units and insufficient resources and capacity to tackle those crimes. Only 7% of countries (two out of the 29) reported that they have set up dedicated units to investigate CSA, including technology-facilitated CSA [5]. These numbers are problematic given the global nature of the internet and the ease of using VPN services to change the location of access (as an illustration, 93% of all reports to the NCMEC's CyberTipline in 2021 were tied to locations outside of the US, and those mostly indicated locations where CSAM files had been uploaded).

The lack of universal standards for categorizing and penalizing CSAM and the differences in the regulation of CSAM offenses (e.g., the age limit specified to make CSAM an offense under the law may range from 14 to 18 years of age) have hampered the possibility for global cooperation among countries and national law enforcement agencies [112] [113]. Although heavily advocated for, a global system of standards for identifying, analyzing and classifying CSAM does not exist yet, and international collaboration between jurisdictions is cumbersome. The issue is illustrated by an interviewee who works as a criminal investigator:

"*Most of the service providers have headquarters abroad, mostly in the USA. The police can ask for basic subscriber information (BSI) out of the information given by people when they establish an online profile. The police can obtain this information without a warrant. However, the situation becomes much more difficult when the police try to obtain information on the content connected to a certain profile. Then, the police must obtain a warrant from a regional public prosecutor's office, which is then sent to the Director of Public Prosecutions, which then goes to the Ministry of Justice, then to the Ministry of Foreign Affairs, which sends the case to the US Ministry of Foreign affairs, from where it is transmitted to state authority entities, then to local authority bodies, which then apply US regulations compliance checks (in California, for example). In Norway, we may have different regulatory frameworks than in the US, but the case must be punishable in both countries to be eligible. In line with US laws, the Norwegian police must document that the content connected to those profiles is related to the criminal offense. It is not their problem [California's regulators'] if the Norwegian police cannot document the relationship between the case and the profile because they cannot access the content associated with that profile. The Norwegian police are fully dependent on cooperation with service providers and their rapid response.*"

Similar issues of *regulatory ambiguity* also occur at the national level. Interviewees working for Norwegian law enforcement note the overall lack of ability to follow CSA trends over time, particularly those trends that concern different technological solutions due to the weaknesses of the penal code in distinguishing online from offline offenses and the technological sources used. The result is that police investigators are uncertain about how to label certain offenses, which leads to subjectivity in coding. Moreover, insufficient sharing of investigative methods across regions in Norway affects the clearance rate (oppklaringsprosent), while the existing CSA units experience high turnover of officers, which creates knowledge gaps. Hence, available statistics may not represent the true state of practice due to the subjective nature of case registration. Nevertheless, Figure 5 illustrates CSA-related penalty codes in the police database of cases (Strasak) and the trends in these cases in the period from 2017 to 2021, indicating that the representation or depiction of CSAM represents the largest part of the total of offenses (code 1470).

4.1.2 Lack of legal enforcement by electronic service providers

The second important legal challenge in CSAM prevention concerns misconceptions about what is voluntary and mandatory under the law as far as the responsibility of ESPs to report CSAM they find on their platforms. In the US, federal law (18 USC 2258A) requires that US-based ESPs report CSAM they detect on their platforms to the clearinghouse (NCMEC); however, the duties of these ESPs and non-US ESPs toward local authorities outside of the US have been mixed. In Europe at large, the reporting of online CSAM is voluntary, and there are no national or European equivalents to the clearinghouse with its mandatory reporting obligations. The lack of clear regulatory guidance and regulatory bodies to oversee policies has resulted in a situation is which the practice of ESPs relies on blocking or deleting

CSAM when this content is in breach of their internal community rules and algorithms that are not transparent for regulators and law enforcement.

Moreover, US firms are legally protected from liability for content posted on their platforms or services (Section 230 of the 1996 Communication Decency Act), and there is no legal mechanism mandating or forcing firms to actively search or scan for this type of content on their services; rather, the system in the US (as well as in the rest of the world) depends on "good Samaritan" voluntary actions by (some) ESPs. The legal grounds on which service is refused or content is removed from platforms depend on the internal reinforcement of a firm's own code of conduct, and there is no clear guidance about what constitutes best practices or whether the firm must use some recognized detection tool [1]. This lack of guidance contributes to the variability in the propensity to report and a lack of clear standards for data quality. This problem is exacerbated by the fact that it is easy to create multiple and fake accounts to access online services and that, according to current legal obligations, ESPs do not need to keep their records (IP addresses) for a longer period of time. In Norway, in 2021, the regulation that mandated that ESPs keep their records for 21 days was changed to extend that timeframe to one year [114]. Indeed, this information is critical in the investigation of CSA-related online offenses. In 2021, approximately 30% of CSA-related cases were classified in the STRASAK database as unresolved due to various reasons often related to the lack of information and missing traces (for example, because companies did not keep records over time). This issue is illustrated by an interviewee who works in the national crime unit:

> "*The challenge is that electronic service providers operate in such a way that they delete or block an offending account on the grounds that it breaks their service terms or community standards. When the profile is deleted, all incriminating evidence is gone. Police can only penalize offenses for which there is evidence, and for that to happen they need to ask for information, but they cannot do so if the information has been deleted or is not available.*"

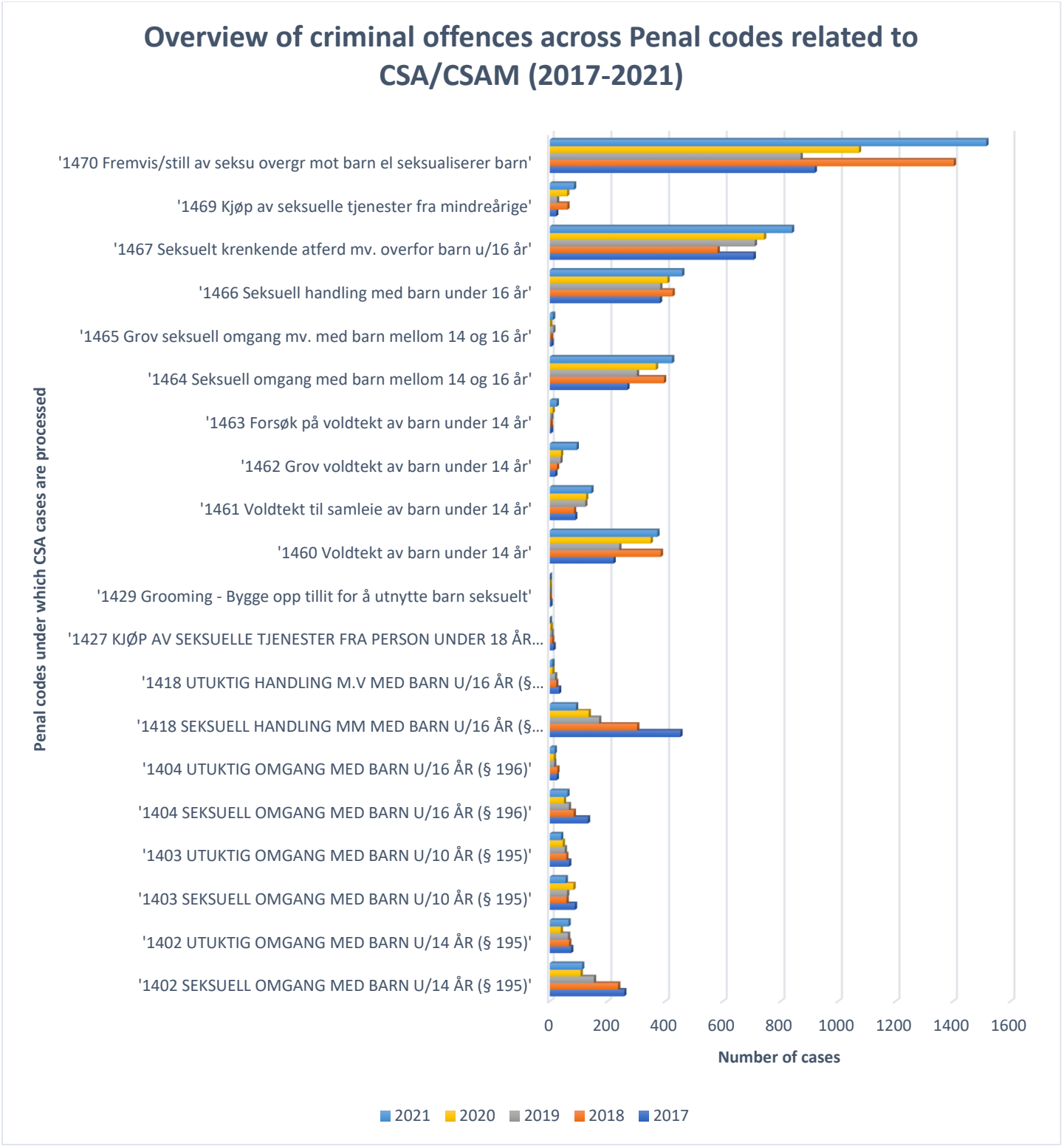


Figure 5: Overview of codes used for offenses related to CSA and trends in the occurrences of these offenses from 2017 to 2021. Source: STRASAK database, Seksjon strategi, plan og utvikling i virksomhetsstyringsstaben, Trøndelag police district, 2022.

To date, Norway does not have a mandatory reporting body that oversees ISPs and platforms or firms through which user-to-user messaging occurs. Attempts to change the system in the US and Europe are still ongoing, mostly through proposals to change the legislation such as the EU's Better Internet for Kids (BIK+) and the EARN IT Act in the US, which aim to impose more stringent requirements on ESPs. In 2022, the European Commission proposed a new Strategy for Better Internet for Kids (BIK+), focusing on the online digital experiences of children [7]; the main features of this new strategy is that both age-appropriate design and the reporting of content are made mandatory. This change moves regulatory conditions toward mandatory reporting to a central European clearance house similar to the NCMEC in the US. It is uncertain whether Norway will immediately follow and adopt the new EU regulation and/or make it mandatory for firms operating in Norway to report to the European clearing body. Not adopting these regulatory changes creates the risk that CSAM material from EU servers could move to nonmember states where regulation is still adopted on a voluntary basis.

We note that both these proposals that aim at changing the regulation in the Us and the EU are still being debated and highly contested by ESPs and parties that fear that these developments may hurt the privacy of users, freedom of speech and the tendency of people to use end-to-end encryption.

The second related issue is the question of who should manage the hotline or a clearinghouse where CSA and CSAM is being reported in Norway. The current operational structure in Norway places reporting (tiplines) under the jurisdiction of the police (Kripos and police districts) rather than under the authority of independent civil society organizations such as NGOs (as is customary in Denmark, Finland, the US and the UK). The concern is that reporting to the police rather than to an independent institution creates a chilling effect limiting people's willingness to report. Moreover, the benefits and drawbacks for Norwegian citizens and firms of having the main reporting clearinghouse hosted outside of Norway (e.g., in the EU) are unclear.

4.1.3 Legal challenges concerning solutions using artificial intelligence (AI)

The final legal and regulatory challenge that we discuss in this report involves concerns about the use by law enforcement of automated AI systems. The issue is related to the lack of harmonized standards in applying high-risk AI systems to surveil citizens' activities online [115]; moreover, a debate has emerged about the proposed legislation (i.e., AI Act) concerning the use of AI by law enforcement. The issue that has been debated by both regulators and the general public is whether scanning for CSAM that is located on personal devices infringes on basic human rights and privacy laws [116] [117]. This general fear of surveillance has been exacerbated by lay people's aversion toward making automated decisions through AI applications in domains having to do with morality [118], such as policing. The issue primarily concerns fears that AI systems (relative to humans) are still not proficient at recognizing human uniqueness, identifying contexts and empathizing with circumstances, which may lead to increased fear of false positives (i.e., regular content being wrongfully identified as CSAM). For example, watchdog moms and parent groups that voluntarily survey and report online abuse on popular social media platforms, warn about the faulty algorithms used by ESPs that tag educational videos as CSAM and about the new ways in which predators learn to avoid automated detection by ESPs [72].

Fears against automated solutions to CSAM feed on the heightened debate in public and social media on obscure uses of algorithms and the lack of consensus on whether humans or AI should be used for CSAM content surveillance. This issue has become important, showing Apple's recent failed attempt at introducing NeuralHash, a proprietary hashing algorithm that was to be implemented on Apple's hardware. After announcing its intent to launch the technology in September 2021, in the face of harsh criticism from the public regarding fears of surveillance, invasion of privacy and the risk for false positives, Apple postponed the launch "over the coming months to collect input and make improvements", in spite of the fact that there were only 3 false positive collisions in a test of 100 million images [129].

Our interviewees, both from civil society and the private sector, highlighted their strong fears in the face of high numbers of false positive results in the current use of AI as well as the potential for racial, ethical and gender biases and discrimination in these algorithms (known as algorithmic biases [119]). The UN have initiated guidelines to harmonize the ways in which law enforcement applies AI to echo these concerns and have warned about potential biases in current algorithms, which are trained on data that are biased against certain groups and lenient toward others [56]. We acknowledge that due to length limitations, we have not been able to delve fully into these issues in this report, but we note them here as they are likely to become part of some of the critical legal and regulatory debates in the near future, as it becomes unavoidably needed for law enforcement to use and apply the AI methods we discussed in Section 3.7.

4.2 Cooperation between the private and public sectors, firms and law enforcement as critical to CSAM identification and penalization

As noted throughout this report, online providers of services, ESPs, and financial institutions that follow money flows have critically collaborated with law enforcement in two domains. First, ESPs have gained the unprecedented ability to provide state-of-the-art technical solutions to identify and fight CSA online; thus they can assist in identifying offenders/victims and in preventing the sharing of CSAM. Second, as discussed in Section 4.1.2, there has been a lack of industry-wide commitment and no standardized duty applying to the industry at large [28].

Firms' goals of engaging in social causes (e.g., preventing sexual abuse of children) may come in conflict with their legal and strategic goals of protecting their customers' privacy and enhancing customers' experiences and satisfaction. The report by Thorn [1] highlights concerns identified by managers in in-depth interviews: most companies worry about drawing attention to CSA on their service platforms for fear that their brand become associated with this content, rather than people being tuned in to an industry-wide social problem. As one interviewee indicated, "*who wants to be associated with that? We do not want our customers to even think about this in relation to our brand (but we still want to get rid of it through our back office activities)".* Indeed, many firms are reluctant and unwilling to raise these issues.

On the other hand, firms are intrinsically motivated to protect their brand and nurture customers' trust. The main motivation for the firms that we have investigated and that have proactively engaged in scanning for abusive materials on their service platforms is the need to protect the brand and customers' safety. Some of the interviewed managers felt that enhancing safety is an important competitive strategy for the future.

> "*At the same time, we want our customers to know our services are safe and we are not a hub for such material; so we are willing to go an extra mile to secure that.*" (Interviewee, software company)

> "*This firm sees the safety of children, even at the cost of privacy or profitability, as the main strategy!"* (Interviewee, online entertainment service)

Our analysis reveals that in Norway, very few ESPs directly collaborate with the police on CSAM prevention. The main reasons include the fact that providers report to their headquarters' country (typically the USA) rather than locally and that many medium and smaller providers lack systems, skills and financial resources to scan their services. These gaps have led to a situation in which most of CSAM detection activities depend on the NCMEC's reports (discussed next).

4.2.1 Collaboration with electronic service providers and Norwegian law enforcement

Although interviewees working for law enforcement felt that the cooperation between law enforcement and ESPs (particularly international ones) could be improved, they also acknowledged that these external reports represent the main source for leads about online CSA. Figure 6 provides an overview of the leads contributed by various ESPs on which the police has acted. Because of their large pool of customers, Facebook, followed by Snapchat and Instagram, has filed the greatest number of reports with the Norwegian authorities.

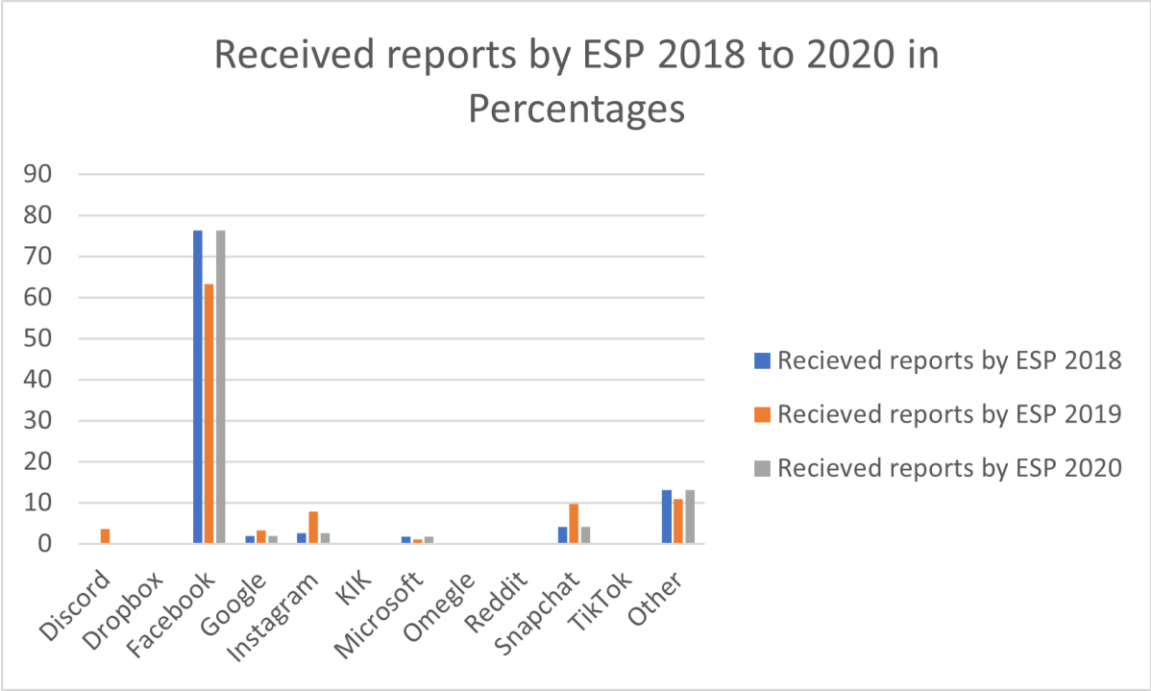


Figure 6: Number of reports filed by electronic service providers with Kripos from 2018 to 2020. Source: Kripos, NC3 report, 2022.

For deeper insights, Table 2 provides an overview of the yearly number of reports that the NC3 unit at Kripos has received from various ESPs. The percentage of imported reports indicates the share of the total number of received cases that have been imported for further investigation by law enforcement in Norway.

Table 2: Number of reports received from ESPs over several years. Source: Kripos, NC3 internal materials. 2022.

Received from NCMEC	2018	Imported	2019	Imported	2020	Imported	2021	Imported
Discord	0	0.0%	247	91.9%	65	90.8%	122	81.1%
Dropbox	7	100.0%	13	100.0%	36	88.9%	139	73.4%
Facebook	7982	6.6%	4341	11.1%	3819	20.2%	2013	14.0%
Google	197	70.6%	220	77.3%	312	71.5%	427	80.1%
Instagram	263	13.3%	535	21.3%	793	22.7%	341	19.1%
KIK	0	0.0%	0	0.0%	62	98.4%	114	86.8%
Microsoft	175	86.9%	78	89.7%	154	81.2%	207	76.8%
Omegle	23	47.8%	17	35.3%	170	28.8%	405	10.1%
Reddit	4	75.0%	1	0.0%	8	25.0%	79	53.2%
Snapchat	436	84.9%	669	79.5%	1082	67.0%	3105	64.3%
TikTok	0	0.0%	3	100.0%	64	82.8%	327	53.8%
Øvrige	1376	16.2%	744	41.7%	474	56.8%	571	42.6%
Totalt	10463		6868		7039		7850	

Overall, Table 2 shows great differences across ESPs in terms of the number of imported cases and the quality of information received from these reports. The columns that indicate these percentages show that although some service providers report a lower total number of violations, the quality of the information they provide, upon which the investigators depend to start cases, is significantly higher. For example, while Facebook sends more than 75% of all reports, only between 10 to 20% of these reports contain sufficient evidence to start an investigation. In contrast, leads provided by KIK, Microsoft or Dropbox are imported at the rate of 75 to 100%.

4.2.2 Cooperation with financial institutions based on anti-money laundering regulation

Online child sexual abuse and exploitation are often underpinned by financial transactions from offenders who buy CSAM or order live streaming [46]. Even new forms of CSAM, such as live streaming, are typically funded with payments relying on various financial instruments [45]. Often, offenders make payments using various anonymous service providers, financial institutions and cryptocurrencies to avoid drawing suspicious attention [45]. Therefore, utilizing data held by the global network of financial intelligence units provides opportunities to enhance strategic and tactical intelligence efforts to combat online CSA. Payments take place through both anonymized and more traditional options, such as online payment services. According to Europol, perpetrators have increasingly used cryptocurrencies to pay each other for sexual abuse material, while more traditional payment services have been increasingly used in connection with on-demand livestreamed abuse [14] [120].

In Norway, a private–public cooperation [121] (The OPS AT project) was launched in August 2021 to strengthen the national collaboration between the reporting entities and authorities involved in the prevention and uncovering of money laundering and financing terrorism. The overall objective has been to better coordinate and share information between the financial industry and public authorities. Law enforcement members include Økokrim (the National Authority for Investigation and Prosecution of Economic and Environmental Crime), which is the main source of specialized skills for the police and the prosecuting authorities focusing on economic and financial crimes.

Financial indicators and keywords linked to the online streaming of CSA can be used by the Finance Intelligence Unit (FIU) in financial institutions to proactively identify transactions likely to be linked to online streaming of CSA within their dataset. Our analysis and interviews show that Økokrim and its FIU [122] have been making progress in their cooperation with the financial sector to identify the CSA activities of Norwegian citizens based on transnational payments that may be directed to offenders'' accounts abroad, particularly known accounts in the Philippines (the information stems from internal reports and interviews with both police investigators and managers in the financial sector).

In the period 2017-2021, Økokrim filed 1277 suspicious transaction reports (STRs) related to suspected online CSA. The number of reports filed has risen since 2017, as illustrated in Figure 7, reaching a peak in 2021 with 459 reports [123]. This increase in the number of identified cases can be due to the increased awareness of financial transactions in these cases, crime indicator lists prepared by the FIU and increased media coverage that raised awareness among firms. The fact that the Norwegian FIU's has cooperated with other national FIUs through the Egmont group has reportedly resulted in information

being shared at a higher rate [122]. The Egmont Group projects to increase financial intelligence sharing focused specifically on online streaming due to the development of criminal business models specifically established for online streaming [122]. Nevertheless, our interviews with financial sector experts and law enforcement officers show that CSA prevention and detection is not the main task for financial fraud units (which focus predominantly on money laundering and the financing of terrorism); therefore, CSA may not have received full attention and would require more skilled staff.

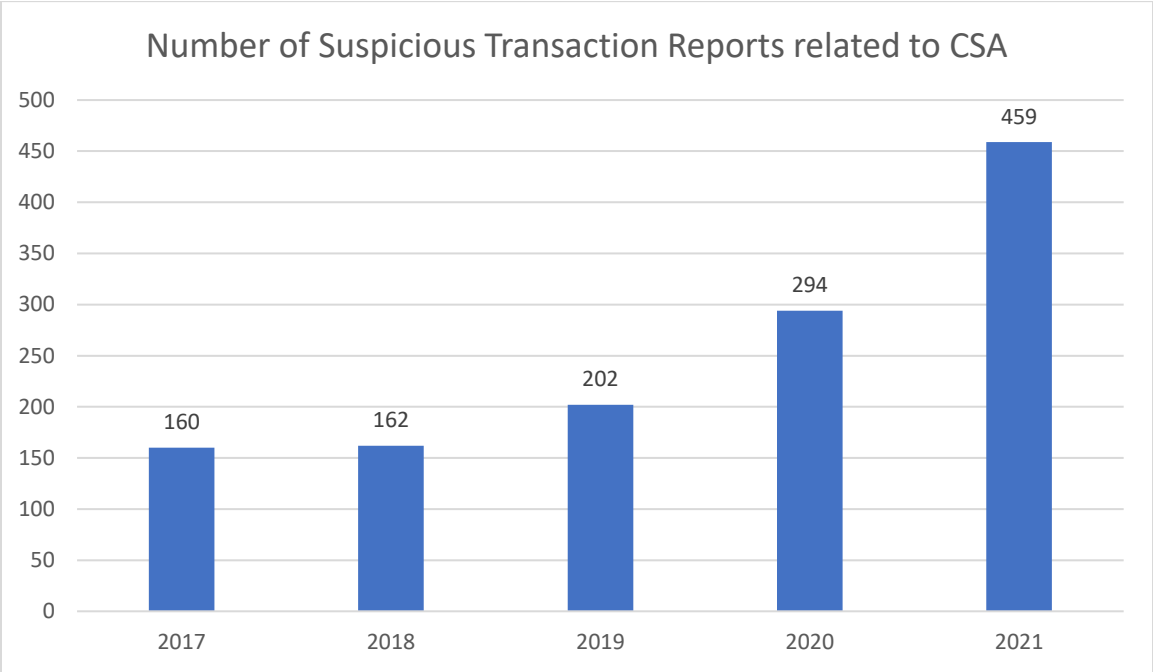


Figure 7: Number of suspicious transaction reports (STRs) filed by financial institutions in Norway per year. Source: Økokrim. Årsrapport 2021. Enheten for finansiell etterretning [123]. Page 23.

As a result of a joint effort involving banks, which understand the situation, and of a collaboration with the FIU analysis team, the money could quickly be traced to identify criminal payments and stop those. Information from investigations and intelligence relating to payment transfers made by Norwegian nationals to known facilitators of sexual abuse on demand indicates that much of this activity goes undetected. Our investigation indicates that it is difficult to delineate financial transactions related to payments made for online streaming from payment made for adult sexual content, fraudulent activity or other CSAM-related material, such as images, because these transactions have similar financial profiles. Similarly, the use of live streaming that has been commissioned by a person in a Global North country and committed against a child in a Global South country can be detected only when payments are made through regular means and to the benefit of a known offender. The use of cryptocurrency and other privacy-enhancing techniques for payments has deterred efforts to identify financial transactions related to CSA.

4.2.3 Firms' warning that cooperation with law enforcement should be reciprocal

In this report, we also want to present limitations and bottlenecks firms face that burden their stronger engagement with CSAM prevention. One of the main complaints firms make is that when they voluntarily collaborate with law enforcement, communication is one-directional, i.e., from firms to law enforcement. Firms indicate that getting feedback from law enforcement and explanations about the concrete modus operandi of offenders would make it easier for them to adjust their own algorithms and methods.

However, all our respondents from the industry and some law enforcement officers have indicated that due to confidentiality reasons, the legal obligations to fully protect information during investigation and complicated procedures related to 'intelligence data' (etterretningsdata), the police's communication with firms on how to improve their detection efforts has been minimal. The hindrances encountered in this collaboration are seen primarily in the ways in which the work has been structured and reflect the fact that the protection of information is highly sensitive and that the police is afraid of sharing its intelligence. An interviewee from the industry explained the issue in the following way:

> *"I have to say that I have been given free reins by firms and resources to set up a system for the detection of CSA, but I met quite some resistance, specifically from certain police authorities. What happens is that they say it is not possible to share any information with us. However, it is important to have examples of cases, profiles and patterns that they could share with us, so that we can create systems; however, no one dares to share the information, and I have spoken to all of them. They do not come back to us with concrete information or examples that could help set up flags in the system, probably because of these rules about sharing sensitive information about people and protecting the privacy of the people under investigation."*

Our analysis of the challenges that interviewees from the public sector have outlined showed the following:

- High-level management in firms whose services may be subject to CSAM sharing does not highlight any systematic strategies publicly for fears of raising the awareness of users.
- Currently, few firms lead initial efforts at combatting CSA globally and locally, and those are typically the largest players in the industry, such as those involved in technology services and financial and telecommunication institutions; however, a vast number of other services currently have insufficient knowledge and resources devoted to this goal.
- While management in firms that deal with CSA or CSAM encourages detection and removal of this material, the initiatives, methods and approaches are bottom-up and driven by operational units that often employ ex-police officers/investigators and data scientists who are overburdened with the volume of the task and lack of guidelines.
- Current developments rely on automated techniques, AI applications and machine learning, which, although developing rapidly, still suffer from significant false positive and algorithmic biases in predictive techniques. Due to the increased fear of bias, substantive investments in method

development and a high level of skills are needed, but most firms still rely on hash matching techniques despite their weaknesses.

Conclusion

The Lanzarote Convention [125] on the protection of children against sexual exploitation and sexual abuse written by the Council of Europe (ratified by Norway, among other state parties), as well as the Norwegian national strategy [13] for coordinated efforts in preventing and combating internet-related abuse against children, mandate the criminalization of all kinds of sexual offenses against children, whether offline or online. However, protecting children and other vulnerable groups online may require sacrifices in other areas and implicate other stakeholders (e.g., infringement on privacy by government or corporate surveillance, infringement on business algorithms and trade secrets, or harm that may be done to the user-brand relationship between firms and their customers). Therefore, the reduction of CSA online is an endeavor that brings together multiple stakeholders, including law enforcement, the industry, civil society, parents and children themselves [45]. This collaboration means that reducing instances of CSA online is neither the sole responsibility of any organization nor a task that law enforcement can undertake alone. This report has provided an overview of the ways in which technology in general and diverse technological solutions in particular impact the possibilities of accessing and sharing CSA online and the opportunities perpetrators have to establish contacts with victims.

Our review of the available literature, analysis of existing empirical evidence from police records and interviews with various stakeholders show that digital solutions are significant because

1. they exacerbate the problem of CSA and CSAM sharing by expanding the opportunities perpetrators have to contact children through gaming and social media platforms and to share large amounts of material (predominantly through peer-to-peer networks), and
2. they deter law enforcement from identifying perpetrators because several of these technological solutions allow perpetrators to mask their identity and the digital traces of their activities (e.g., VPN connections, dark web, end-to-end encryption, cryptocurrency payments, XR and deepfake morphing allow for anonymity and/or make the identification of digital footprints cumbersome).
3. the technology used to identify hashes (the digital fingerprints of CSAM) and machine learning solutions that allow for the identification of new CSAM represent the main countermeasures against online CSA. Using technology that allows the rapid scanning of a large volume of data is the only way forward in counteracting large volumes of content and facing the technological advancements emerging in CSAM distribution.

Through our analysis of Norwegian law enforcement activities, we have identified major trends in the technology used, which corresponds to the challenges identified in studies of law enforcement in other countries across the globe [25] [80] [113]. Overall, participants from both law enforcement and the judicial system revealed that [113] they feel they are often several technological steps behind

perpetrators in terms of the technologies that have developed to capture or share CSAM. As a peak in CSAM cases occurred during the COVID-19 pandemic, this technological lag has been particularly exacerbated [80].

Our analysis shows that CSAM hosted on websites and distributed through server systems represents the largest volume of known CSAM in circulation. The detection tools that (largest) ESPs and NGOs use are targeted toward identification of the known CSAM, particularly on websites and file-hosting services. The main technology used for the identification of CSAM relies on the matching of digital footprints (hashes). This technology works well to identify known images and is slightly less effective in identifying video materials, but it cannot identify new and previously unknown material. Only sophisticated machine learning and AI can go through such data and identify new cases of CSAM.

Our interviews with police officers, civil society organizations and firms about these technological trends as they relate to CSAM in Norway and Europe revealed insight from a global survey of police officers from 39 countries who work on CSA and CSAM cases [80]. The survey revealed that 80% of police officers reported a (considerable or moderate) increase in perpetrators attempting to contact children online, whereas 60% of police officers reported an increase in self-produced CSAM. Our findings indicate an increase in CSA-related cases from 2017 to 2021, an increase in the number of external reports of CSAM that concern Norwegian citizens and IP addresses and an increase in the number of suspicious financial transactions that are related to CSA. These trends indicate an overall increase in the threat of CSA but also a potential increase in the ability of ESPs and law enforcement to track and report online CSA.

However, similar to what we found in our conversations with officers, we found that as much as half of all officers polled in a global survey felt unable to estimate the trends related to the dark web and live streaming activities in their work [80]. New technological developments that facilitate anonymization and increase the protection of privacy (as in point 2 above) enhance the difficulties of third parties (including ESPs, law enforcement or others) in monitoring transactions and sharing information. The extent to which these developments currently affect law enforcement's ability to track CSA can be summarized by the following statement by a police officer we interviewed:

> *"If perpetrators use VPN, they are to a large extent anonymized and can conduct criminal activities outside of the reach of the authority of law enforcement. This is a great challenge for the police. Around 80% of the perpetrators who shared CSAM in the 2017-2018 period could be identified by the police; now, the rate has decreased to 40% because offenders use services and technological solutions that hide their identity. Identifying perpetrators has become more difficult for police investigators.*"

This statement echoes the NCMEC's estimation that Meta's implementation of end-to-end encryption will reduce the number of CSAM reports by more than 50% [25]. We believe the impact may be even greater given that Meta currently contributes more than 93% of all reports (primarily from the Facebook Messager system that Meta has attempted to make end-to-end encrypted).

Since technological development cannot be stopped, the need for countermeasures has increased. Moreover, with this need comes the challenge of balancing safety and privacy. The prevalence of

smartphones and social media has created a sharing culture in which sharing images and videos with others, both friends and strangers, is an integral part of everyday life [14]. These social activities are protected by privacy laws and freedom of speech. However, at the same time, these civil and political rights must not come at the cost of social and cultural rights such as the right to social protection, to an adequate standard of living and to the highest attainable standards of physical and mental well-being [124].

Given the importance of collaboration between the private sector, civil society and law enforcement in preventing and punishing CSA online, two conclusions may be drawn from this report:

- The rapid development of bespoke technological tools in the industry largely outpaces the skills and the financial and human resources of law enforcement. However, bespoke tools are often used as proprietary tools or for commercial purposes and are not widely made available to law enforcement (or to small and medium-sized firms). Currently, there is no mandatory requirement for non-US ESPs to report detected CSAM; even for US ESPs, there are no mandatory requirements to scan all content for CSAM, and the industry deletes accounts internally, which renders any evidence of abuse unavailable. Through regulation, legislators should require that ESPs proactively scan their digital services and oblige them to report CSA instances.
- The collaboration between trusted industry partners (such as ESPs) and law enforcement must be encouraged and enabled through the development of cooperation frameworks and standards that benefit both sides in the development of effective strategies. Currently, law enforcement efforts suffer from a lack of technical skills, technological advancements and tools that would increase efficiency. On the other hand, the development of sophisticated tools that would reinforce such efficiency suffers from a lack of cooperation in the sharing of information/intelligence. Legal clarifications of standards of cooperation must enable this collaboration.

We conclude that further developments are greatly needed to prevent and investigate CSA online; these developments will critically depend on the two-way collaboration of firms (who develop tools and apply CSAM prevention techniques in their services) and law enforcement (who needs to give feedback on the way they train on the models and bespoke tools). Given the loose and inconsistent regulatory frameworks currently in place that allows most firms to avoid addressing these issues proactively, these collaborations will have to be driven by increased regulation. Given the lack of access to the proprietary services of ESPs, law enforcement must rely on ESPs' reports (which in many instances represent 90% of all CSAM detection cases) and hotlines such as the InHope network in Europe. Finally, since firms face trade-offs between protecting people's safety and violating their privacy and the satisfaction of consumers and since many small- and medium-sized companies currently do not have the capabilities and resources to scan CSAM, the enforcement of strategies aiming to improve the safety of children must come from regulators who must define the best practices as well as tools that ESPs and law enforcement should use and make them widely available.

We hope that this report may contribute to efforts made to combat CSA online and create a safer environment for our children.

References

[1] Thorn, “The Intersection of Technology and Child Sexual Abuse,” *Thorn*, 2020. https://www.thorn.org/child-sexual-exploitation-and-technology/ (accessed Mar. 17, 2022).

[2] A. L. Newton, “An Evaluation of the Rise of Online Sexual Exploitation of Children and Technology: How the Past Three Decades Speak to Future,” PhD Thesis, 2021.

[3] D. M. Hughes, “The use of new communications and information technologies for sexual exploitation of women and children,” *Hastings Women’s LJ*, vol. 13, p. 127, 2002.

[4] E. Martellozzo and J. DeMarco, “Exploring the removal of online child sexual abuse material in the UK: Processes and practice,” *Crime Prev Community Saf*, vol. 22, no. 4, pp. 331–350, Dec. 2020, doi: 10.1057/s41300-020-00099-2.

[5] United Nations Children’s Fund, “Ending Online Sexual Exploitation and Abuse: Lessons learned and promising practices in low- and middle-income countries.” Dec. 2021. Accessed: Feb. 05, 2022. [Online]. Available: https://www.unicef.org/media/113731/file/Ending%20Online%20Sexual%20Exploitation%20and%20Abuse.pdf

[6] National Center for Missing and Exploited Children, “CyberTipline Data,” *National Center for Missing & Exploited Children*, 2022. http://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.html (accessed May 19, 2022).

[7] European Commission, “A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+),” European Commission, COM(2022) 212 final, Nov. 2022. Accessed: Nov. 30, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0212&from=EN, and, d69a3a5e-8b3e-66cc-d3de-a4212e3c6e9b (betterinternetforkids.eu)

[8] Internet Watch Foundation, “The Annual Report 2021,” 2021.

[9] Medietilsynet, “Nakenbilder og porno,” *Medietilsynet*, May 18, 2021. https://www.medietilsynet.no/digitale-medier/barn-og-medier/foreldreguide/ (accessed Nov. 30, 2022).

[10] Thorn, “We Build Tools to Defend Children From Sexual Abuse | Thorn,” *We Build Tools to Defend Children From Sexual Abuse | Thorn*, Nov. 30, 2022. https://www.thorn.org/ (accessed Nov. 30, 2022).

[11] Canadian Centre for Child Protection, “Survivors’ survey - Executive summary 2017,” Canadian Centre for Child Protection, 2017. Accessed: Nov. 30, 2022. [Online]. Available: https://protectchildren.ca/pdfs/C3P_SurvivorsSurveyExecutiveSummary2017_en.pdf

[12] European Commission, “EU strategy for a more effective fight against child sexual abuse.” European Commission, Jul. 24, 2020. Accessed: Dec. 04, 2022. [Online]. Available: https://home-affairs.ec.europa.eu/system/files/2020-07/20200724_com-2020-607-commission-communication_en.pdf

[13] Justis- og beredskapsdepartementet, “Forebygging og bekjempelse av internettrelaterte overgrep mot barn.” Justis- og beredskapsdepartementet, Aug. 15, 2021. Accessed: Nov. 30, 2022. [Online]. Available: https://www.regjeringen.no/contentassets/2915ff68eb2849edb3218055be32d8cb/strategi-mot-internettrelaterte-overgrep-mot-barn_uu.pdf

[14] Kripos, “Online Sexual Exploitation of Children and Young People.” Aug. 11, 2019. Accessed: Feb. 06, 2022. [Online]. Available: https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/seksuelle-overgrep-mot-barn/online-sexual-exploitation-of-children-and-young-people.pdf
[15] Wikipedia contributors, “IP address — Wikipedia, the free encyclopedia.” 2022. Accessed: Nov. 30, 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=IP_address&oldid=1119302818
[16] Wikipedia contributors, “Dark web — Wikipedia, the free encyclopedia.” 2022. Accessed: Nov. 30, 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Dark_web&oldid=1106032026
[17] Byju’s, “Cryptocurrency: Definition, Advantages & Disadvantages,” *BYJUS*, 2021. https://byjus.com/current-affairs/cryptocurrency/ (accessed Nov. 30, 2022).
[18] B. G. Westlake, “The Past, Present, and Future of Online Child Sexual Exploitation: Summarizing the Evolution of Production, Distribution, and Detection,” in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, T. J. Holt and A. M. Bossler, Eds. Cham: Springer International Publishing, 2020, pp. 1225–1253. doi: 10.1007/978-3-319-78440-3_52.
[19] GCHQ Government Communications Headquarters, “A thematic overview of how the internet facilitates the distribution of Child Sexual Abuse Material.” GCHQ Government Communications Headquarters, 2022.
[20] M. Liberatore, R. Erdely, T. Kerle, B. N. Levine, and C. Shields, “Forensic investigation of peer-to-peer file sharing networks,” *Digital Investigation*, vol. 7, pp. S95–S103, Aug. 2010, doi: 10.1016/j.diin.2010.05.012.
[21] C. M. S. Steel, “Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms,” *Child Abuse & Neglect*, vol. 44, pp. 150–158, Jun. 2015, doi: 10.1016/j.chiabu.2014.12.009.
[22] WeProtect Global Alliance, “Estimates of childhood exposure to online sexual harms and their risk factors,” Oct. 19, 2021. https://www.weprotect.org/economist-impact-global-survey/ (accessed Nov. 30, 2022).
[23] ECPAT International, “Trends in Online Child Sexual Abuse Material.” Apr. 2018. Accessed: Sep. 05, 2022. [Online]. Available: https://ecpat.org/wp-content/uploads/2021/05/ECPAT-International-Report-Trends-in-Online-Child-Sexual-Abuse-Material-2018.pdf
[24] C. Steel, E. Newman, S. O’Rourke, and E. Quayle, “Technical Behaviours of Child Sexual Exploitation Material Offenders,” *JDFSL*, 2022, doi: 10.15394/jdfsl.2022.1794.
[25] C. Teunissen and S. Napier, *Child sexual abuse material and end-to-end encryption on social media platforms: an overview*. Australian Institute of Criminology, 2022. doi: 10.52922/ti78634.
[26] Meta, “Child Endangerment: Nudity and Physical Abuse and Sexual Exploitation,” *Community Standards Enforcement | Transparency Center*, 2022. https://transparency.fb.com/data/community-standards-enforcement/child-nudity-and-sexual-exploitation/facebook/ (accessed Nov. 30, 2022).
[27] H.-E. Lee, T. Ermakova, V. Ververis, and B. Fabian, “Detecting child sexual abuse material: A comprehensive survey,” *Forensic Science International: Digital Investigation*, vol. 34, p. 301022, Sep. 2020, doi: 10.1016/j.fsidi.2020.301022.
[28] Child Dignity Alliance, “Technical Working Group Report - Child safety.” 2018. Accessed: Nov. 30, 2022. [Online]. Available: https://static1.squarespace.com/static/5a4d5d4e7131a5845cdd690c/t/5f15c93f7370541bfad45b15/1595263315850/Child+safety+Report+vD+for+web+%284%29.pdf

[29] National Center for Missing and Exploited Children, “CyberTipline,” *National Center for Missing & Exploited Children*, 2021. http://www.missingkids.org/gethelpnow/cybertipline.html (accessed Nov. 30, 2022).
[30] InHope Association, “Annual report 2021,” InHope Association, 2021. Accessed: Nov. 30, 2022. [Online]. Available: https://inhope.org/media/pages/articles/annual-reports/8fd77f3014-1652348841/inhope-annual-report-2021.pdf
[31] WeProtect Global Alliance, “'Self-generated' sexual material - WeProtect Global Alliance,” Aug. 26, 2022. https://www.weprotect.org/issue/self-generated-sexual-material/ (accessed Nov. 30, 2022).
[32] Internet Watch Foundation, “Self-generated Child Sexual Abuse Online - IWF Annual Report 2021,” 2021. https://annualreport2021.iwf.org.uk/trends/selfgenerated (accessed Nov. 30, 2022).
[33] M. Wood, C. Barter, N. Stanley, N. Aghtaie, and C. Larkins, “Images across Europe: The sending and receiving of sexual images and associations with interpersonal violence in young people’s relationships,” *Children and Youth Services Review*, vol. 59, pp. 149–160, Dec. 2015, doi: 10.1016/j.childyouth.2015.11.005.
[34] Kripos, “Barn som selger egenprodusert overgrepsmateriale: En beskrivelse av fenomenet og omfanget.” Oct. 03, 2021. Accessed: Jun. 16, 2022. [Online]. Available: https://www.politiet.no/globalassets/dokumenter/kripos/seksuelle-overgrep/barn-som-selger-egenprodusert-overgrepsmateriale.pdf
[35] B. O’Donnell, “Rise in Online Enticement and Other Trends: NCMEC Releases 2020 Exploitation Stats,” *National Center for Missing & Exploited Children*, Feb. 24, 2021. http://www.missingkids.org/blog/2021/rise-in-online-enticement-and-other-trends--ncmec-releases-2020-.html (accessed Nov. 30, 2022).
[36] L. M. T. Aanerød and S. Mossige, “Nettovergrep mot barn i Norge 2015–2017,” *NOVA Rapport*, p. 108, 2018.
[37] S. Berggrav, “Hvis du liker meg, må du dele et bilde,” Redd Barna, 2020. Accessed: Nov. 30, 2022. [Online]. Available: https://www.reddbarna.no/content/uploads/2020/12/Hvis-du-liker-meg-m%C3%A5-du-dele-et-bilde.pdf
[38] K. Hegg and P. Lang-Holmen, “Kommuners kriminalitetsforebyggende arbeid med barn og ungdoms nettrisikoer.” Redd Barna, 2020. Accessed: Nov. 30, 2022. [Online]. Available: https://resource-centre-uploads.s3.amazonaws.com/uploads/redd_barna_vi_ser_bare_toppen_av_isfjellet_kommuners_kriminalitetsforebyggende_arbeid_med_barn_og_ungdoms_nettrisikoer.pdf
[39] Kripos, “Ungdrom henges ut på nett: Deling av ulovlig og bekymringsverdig materiale av barn og ungdom.” Jan. 2022. Accessed: Jun. 16, 2022. [Online]. Available: https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/voldtekt-og-seksuallovbrudd/fenomenrapport-exposed-kontoer.pdf
[40] N. Titheradge and R. Croxford, “The children selling explicit videos on OnlyFans,” *BBC News*, May 26, 2021. Accessed: Nov. 30, 2022. [Online]. Available: https://www.bbc.com/news/uk-57255983
[41] R. Swier, “A Look Into OnlyFans: Child Sexual Abuse Material and Trafficking,” *Dr. Rich Swier*, Jun. 12, 2021. https://drrichswier.com/2021/06/12/a-look-into-onlyfans-child-sexual-abuse-material-and-trafficking/ (accessed Nov. 30, 2022).
[42] Internet Watch Foundation, “Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-Streamed Child Sexual Abuse.” 2018. Accessed: Feb. 06, 2022. [Online]. Available: https://www.iwf.org.uk/media/23jj3nc2/distribution-of-captures-of-live-streamed-child-sexual-abuse-final.pdf

[43] Medietilsynet, “Barn og medier 2020: Seksuelle kommentarer og nakenbilder - Delrapport 4.” May 2020. Accessed: Jun. 22, 2022. [Online]. Available: https://www.medietilsynet.no/globalassets/publikasjoner/barn-og-medier-undersokelser/2020/200519-delrapport-4-seksuelle-kommentarer-og-deling-av-nakenbilder---barn-og-medier-2020.pdf
[44] Government Communications Headquarters, “The interim code of practice on online child sexual exploitation and abuse.” Dec. 2020. Accessed: Jun. 10, 2022. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944034/1704__HO__INTERIM_CODE_OF_PRACTICE_CSEA_v.2.1_14-12-2020.pdf
[45] G. Edwards and L. Christensen, *Cyber strategies used to combat child sexual abuse material*. Australian Institute of Criminology, 2021. doi: 10.52922/ti78313.
[46] Egmont Group, “Combatting Online Child Sexual Abuse and Exploitation Through Financial Intelligence - Public Bulletin.” 2020. Accessed: Jan. 06, 2022. [Online]. Available: https://egmontgroup.org/wp-content/uploads/2021/09/2020_Public_Bulletin_Combatting_Online_Child_Sexual_Abuse_and_Exploitation_Through_Financial_Intelligence.pdf
[47] WeProtect Global Alliance, “Global Threat Assessment 2021.” 2021. Accessed: Nov. 30, 2022. [Online]. Available: https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2021.pdf
[48] A. Brown, “Safe from harm: Tackling webcam child sexual abuse in the Philippines,” Mar. 06, 2016. https://www.unicef.org/stories/safe-from-harm-tackling-webcam-child-sexual-abuse-philippines (accessed Nov. 30, 2022).
[49] Interpol, “COVID19 - Child Sexual Exploitation and Abuse threats and trends.pdf.” Sep. 2020. Accessed: Mar. 28, 2022. [Online]. Available: https://www.interpol.int/content/download/15611/file/COVID19%20-%20Child%20Sexual%20Exploitation%20and%20Abuse%20threats%20and%20trends.pdf
[50] ECPAT International, Interpol, and United Nations Children’s Fund, “Disrupting harm in the Philippines - Evidence on online child sexual exploitation and abuse.” 2022. Accessed: Nov. 30, 2022. [Online]. Available: https://www.end-violence.org/sites/default/files/2022-04/DH_Philippines_ONLINE_FINAL.pdf
[51] Internet Watch Foundation, “IWF research on child sex abuse live-streaming reveals 98% of victims are 13 or under,” May 14, 2018. https://www.iwf.org.uk/news-media/news/iwf-research-on-child-sex-abuse-live-streaming-reveals-98-of-victims-are-13-or-under/ (accessed Nov. 30, 2022).
[52] S. Pettifer, E. Barrett, J. Marsh, K. Hill, P. Turner, and S. Flynn, “The Future of eXtended Reality Technologies, and Implications for Online Child Sexual Exploitation and Abuse,” Jun. 2022. Accessed: Jun. 12, 2022. [Online]. Available: https://www.weprotect.org/wp-content/uploads/2022-June-XR-OCSEA-FINAL-PUBLISHED.pdf
[53] H. Heide, “Nå kan hvem som helst lage en troverdig, kunstig stemme,” *Digi.no*, Jan. 29, 2022. https://www.digi.no/artikler/na-kan-hvem-som-helst-lage-en-troverdig-kunstig-stemme/516813 (accessed Nov. 30, 2022).
[54] A. Crochetiere, “Deep-Fake, Real Pain: The Implications of Computer Morphing on Child Pornography | MTTLR,” *Michigan Technology Law Review*, Mar. 2021. http://mttlr.org/2021/03/deep-fake-real-pain-the-implications-of-computer-morphing-on-child-pornography/ (accessed Nov. 30, 2022).

[55] Europol, “The Internet Organised Crime Threat Assessment (IOCTA) 2019,” 2019. [Online]. Available: https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf
[56] United Nations Interregional Crime and Justice Research Institute, “250 Law enforcement representatives and experts from more than 60 countries joined the stakeholder meeting of the ‘AI for safer children initiative,’” *United Nations Interregional Crime and Justice Research Institute*, Jun. 22, 2021. https://unicri.it/News-First-Stakeholder-Meeting-AI-Safer-Children-Initiative (accessed Nov. 30, 2022).
[57] E. Guerra and B. G. Westlake, “Detecting child sexual abuse images: Traits of child sexual exploitation hosting and displaying websites,” *Child Abuse & Neglect*, vol. 122, p. 105336, Dec. 2021, doi: 10.1016/j.chiabu.2021.105336.
[58] C. M. S. Steel, E. Newman, S. O’Rourke, and E. Quayle, “An integrative review of historical technology and countermeasure usage trends in online child sexual exploitation material offenders,” *Forensic Science International: Digital Investigation*, vol. 33, p. 300971, Jun. 2020, doi: 10.1016/j.fsidi.2020.300971.
[59] E. Bursztein *et al.*, “Rethinking the Detection of Child Sexual Abuse Imagery on the Internet,” in *The World Wide Web Conference on - WWW ’19*, San Francisco, CA, USA, 2019, pp. 2601–2607. doi: 10.1145/3308558.3313482.
[60] U.S. Department of Justice, “National Strategy for Child Exploitation Prevention and Interdiction,” Apr. 15, 2016. https://www.justice.gov/psc/national-strategy-child-exploitation-prevention-and-interdiction (accessed May 05, 2022).
[61] M. Latapy, C. Magnien, and R. Fournier, “Quantifying paedophile activity in a large P2P system,” *Information Processing & Management*, vol. 49, no. 1, pp. 248–263, Jan. 2013, doi: 10.1016/j.ipm.2012.02.008.
[62] Kripos, “Internal analysis of peer-to-peer file sharing offences.” Kripos, 2022.
[63] B. G. Westlake and M. Bouchard, “Liking and hyperlinking: Community detection in online child sexual exploitation networks,” *Social Science Research*, vol. 59, pp. 23–36, Sep. 2016, doi: 10.1016/j.ssresearch.2016.04.010.
[64] Internet Watch Foundation, “Total number of CSAM reports - IWF Annual Report 2021,” *Internet Watch Foundation*, 2021. https://annualreport2021.iwf.org.uk/trends/total (accessed Nov. 30, 2022).
[65] B. G. Westlake, M. Bouchard, and A. Girodat, “How Obvious Is It? The Content of Child Sexual Exploitation Websites,” *Deviant Behavior*, vol. 38, no. 3, pp. 282–293, Mar. 2017, doi: 10.1080/01639625.2016.1197001.
[66] K. J. Mitchell, D. Finkelhor, L. M. Jones, and J. Wolak, “Use of Social Networking Sites in Online Sex Crimes Against Minors: An Examination of National Incidence and Means of Utilization,” *Journal of Adolescent Health*, vol. 47, no. 2, pp. 183–190, Aug. 2010, doi: 10.1016/j.jadohealth.2010.01.007.
[67] J. Constine, “WhatsApp has an encrypted child abuse problem | TechCrunch,” *TechCrunch*, Dec. 20, 2018. https://techcrunch.com/2018/12/20/whatsapp-pornography/?fbclid=IwAR1bhm3Zp5OffLeOy-fwdCK2dAjj9O4D8_LpuEEm6lg0r1r3mIHTnnilV-4&guccounter=1 (accessed May 09, 2022).
[68] WhatsApp Help Center, “How WhatsApp Helps Fight Child Exploitation,” *WhatsApp*, Feb. 2021. https://faq.whatsapp.com/154956905959033/?locale=en_US (accessed Nov. 30, 2022).
[69] A. Singh, N. Chandan, R. Pagariya, S. Sahni, S. Sahu, and S. Iyer, “End (-to-end-encrypted) Child Sexual Abuse Material.” 2020. Accessed: Nov. 30, 2022. [Online]. Available: https://www.cyberpeace.org/wp-content/uploads/2022/01/End-to-end-Encrypted-CSAM-2.pdf

[70] G. Mantri, “How can WhatsApp act against child abuse material in encrypted chats? Report suggests,” *The News Minute*, Sep. 29, 2020. https://www.thenewsminute.com/article/how-can-whatsapp-act-against-child-abuse-material-encrypted-chats-report-suggests-134136 (accessed Nov. 30, 2022).
[71] S. Berggrav, “‘Et skada bilde av hvordan sex er’ - Ungdoms perspektiver på porno.” Redd Barna, May 2020. Accessed: Nov. 30, 2022. [Online]. Available: https://resource-centre-uploads.s3.amazonaws.com/uploads/rapport_et_skada_bilde_av_hvordan_sex_er_ungdoms_perspektiver_pay_porno.pdf
[72] S. M. Kelly, “‘Watchdog moms’ on TikTok are trying to keep minors safe | CNN Business,” *CNN*, Jun. 27, 2022. https://www.cnn.com/2022/06/27/tech/tiktok-watchdog-moms-wellness-parenting/index.html (accessed Nov. 30, 2022).
[73] TikTok, “Community Guidelines Enforcement Report Jan - Mar 2022,” *TikTok*, Jun. 30, 2022. https://www.tiktok.com/transparency/en/community-guidelines-enforcement-2022-1/ (accessed Nov. 30, 2022).
[74] P. Biddle, P. England, M. Peinado, and B. Willman, “The Darknet and the Future of Content Distribution,” p. 16.
[75] Europol, “4 arrested in takedown of dark web child abuse platform with some half a million users,” *Europol*, Mar. 05, 2021. https://www.europol.europa.eu/media-press/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-million-users (accessed Nov. 30, 2022).
[76] S. Lu, “What is the dark web and who uses it?,” *The Globe and Mail*, Aug. 19, 2015. Accessed: Jul. 06, 2022. [Online]. Available: https://www.theglobeandmail.com/technology/tech-news/what-is-the-dark-web-and-who-uses-it/article26026082/
[77] G. H. Owen and N. J. Savage, “The Tor Dark Net.” Centre for International Governance Innovation and the Royal Institute of International Affairs, Sep. 2015. Accessed: Jun. 07, 2022. [Online]. Available: https://pure.port.ac.uk/ws/portalfiles/portal/19636608/The_tor_dark_net.pdf
[78] R. S. Portnoff, *The dark net: De-anonymization, classification and analysis*. 2017.
[79] Internet Watch Foundation, “Hidden ‘dark web’ services - IWF Annual Report 2020,” *Internet Watch Foundation*, 2020. https://annualreport2020.iwf.org.uk/trends/international/other/hidden (accessed Nov. 30, 2022).
[80] NetClean, “COVID-10 impact 2020 - A report about child sexual abuse crime.” NetClean, 2020. Accessed: Nov. 30, 2022. [Online]. Available: https://www.datocms-assets.com/74356/1662373830-netcleanreport-2020.pdf
[81] Europol, “The Internet Organised Crime Threat Assessment (IOCTA) 2014,” 2014. Accessed: Jan. 19, 2017. [Online]. Available: https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web.pdf
[82] B. H. Schell, M. V. Martin, P. C. K. Hung, and L. Rueda, “Cyber child pornography: A review paper of the social and legal issues and remedies—and a proposed technological solution,” *Aggression and Violent Behavior*, vol. 12, no. 1, pp. 45–63, Jan. 2007, doi: 10.1016/j.avb.2006.03.003.
[83] M. Balfe, B. Gallagher, H. Masson, S. Balfe, R. Brugha, and S. Hackett, “Internet Child Sex Offenders’ Concerns about Online Security and their Use of Identity Protection Technologies: A Review: Security Internet Technology,” *Child Abuse Rev.*, vol. 24, no. 6, pp. 427–439, Nov. 2015, doi: 10.1002/car.2308.
[84] T. Krone and R. G. Smith, “Criminal misuse of the Domain Name System,” p. 85, 2018.

[85] NetClean, “Hash Values– Fingerprinting Child Sexual Abuse Material,” *NetClean.com*, n.d. https://www.netclean.com/technical-model-national-response/hash-values-fingerprinting-csam/ (accessed May 12, 2022).
[86] B. Westlake, M. Bouchard, and R. Frank, “Comparing Methods for Detecting Child Exploitation Content Online,” in *2012 European Intelligence and Security Informatics Conference*, Odense, Denmark, Aug. 2012, pp. 156–163. doi: 10.1109/EISIC.2012.25.
[87] Interpol, “International Child Sexual Exploitation database,” 2022. https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database (accessed Jun. 22, 2022).
[88] T. Ith, “Microsoft’s PhotoDNA: Protecting children and businesses in the cloud,” *Microsoft News Stories*, Jul. 15, 2015. https://news.microsoft.com/features/microsofts-photodna-protecting-children-and-businesses-in-the-cloud/ (accessed Nov. 30, 2022).
[89] Canadian Centre for Child Protection, “Project Arachnid: Online Availability of Child Sexual Abuse Material.” Aug. 06, 2021. Accessed: Jun. 15, 2022. [Online]. Available: https://www.protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf
[90] NetClean, “Using crawling and hashing technologies to find child sexual abuse material - The Internet Watch Foundation,” *NetClean.com*, Feb. 11, 2019. https://www.netclean.com/2019/02/11/using-crawling-and-hashing-technologies-to-find-child-sexual-abuse-material-the-internet-watch-foundation/ (accessed May 27, 2022).
[91] C. M. S. Steel, “Child pornography in peer-to-peer networks,” *Child Abuse & Neglect*, vol. 33, no. 8, pp. 560–568, Aug. 2009, doi: 10.1016/j.chiabu.2008.12.011.
[92] B. G. Westlake and R. Frank, “Seeing the Forest Through the Trees: Identifying Key Players in the Online Distribution of Child Sexual Exploitation Material,” p. 37, 2016.
[93] B. R. da Cunha, P. MacCarron, J. F. Passold, L. W. dos Santos, K. A. Oliveira, and J. P. Gleeson, “Assessing police topological efficiency in a major sting operation on the dark web,” *Sci Rep*, vol. 10, no. 1, p. 73, Dec. 2020, doi: 10.1038/s41598-019-56704-4.
[94] Internet Watch Foundation, “Top-level domain hopping - IWF Annual Report 2020,” 2020. https://annualreport2020.iwf.org.uk/trends/international/other/toplevel (accessed Jun. 13, 2022).
[95] Wikipedia contributors, “Domain tasting — Wikipedia, The Free Encyclopedia.” 2022. Accessed: Jun. 13, 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Domain_tasting&oldid=1071746199
[96] J. Kharub, “Domain Tasting - A Profiteering Venture,” 2022. https://www.legalserviceindia.com/article/l73-Domain-Tasting---A-Profiteering-Venture.html (accessed Jun. 14, 2022).
[97] Chun-Ying Huang, Shang-Pin Ma, Wei-Lin Yeh, Chia-Yi Lin, and Chien-Tsung Liu, “Mitigate web phishing using site signatures,” in *TENCON 2010 - 2010 IEEE Region 10 Conference*, Fukuoka, Nov. 2010, pp. 803–808. doi: 10.1109/TENCON.2010.5686582.
[98] A. K. Jain and B. B. Gupta, “Phishing Detection: Analysis of Visual Similarity Based Approaches,” *Security and Communication Networks*, vol. 2017, pp. 1–20, 2017, doi: 10.1155/2017/5421046.
[99] M. W. Al-Nabki, E. Fidalgo, E. Alegre, and R. Aláiz-Rodríguez, “File Name Classification Approach to Identify Child Sexual Abuse:,” in *Proceedings of the 9th International Conference on Pattern Recognition Applications and Methods*, Valletta, Malta, 2020, pp. 228–234. doi: 10.5220/0009154802280234.

[100] A. Panchenko, R. Beaufort, and C. Fairon, “Detection of child sexual abuse media on p2p networks: Normalization and classification of associated filenames,” in *Proceedings of the LREC Workshop on Language Resources for Public Security Applications*, 2012, pp. 27–31.
[101] J. Prichard, J. Scanlan, T. Krone, C. Spiranovic, P. Watters, and R. Wortley, “Warning messages to prevent illegal sharing of sexual images: Results of a randomised controlled experiment,” *Trends and Issues in Crime and Criminal Justice*, 2022.
[102] Europol, “Police2Peer,” *Europol*, Sep. 12, 2021. https://www.europol.europa.eu/partners-collaboration/police2peer (accessed Nov. 30, 2022).
[103] J. Wolak, M. Liberatore, and B. N. Levine, “Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network,” *Child Abuse & Neglect*, vol. 38, no. 2, pp. 347–356, Feb. 2014, doi: 10.1016/j.chiabu.2013.10.018.
[104] C. Schulze, D. Henter, D. Borth, and A. Dengel, “Automatic Detection of CSA Media by Multi-modal Feature Fusion for Law Enforcement Support,” in *Proceedings of International Conference on Multimedia Retrieval*, Glasgow United Kingdom, Apr. 2014, pp. 353–360. doi: 10.1145/2578726.2578772.
[105] N. Sae-Bae, X. Sun, H. T. Sencar, and N. D. Memon, “Towards automatic detection of child pornography,” in *2014 IEEE International Conference on Image Processing (ICIP)*, Paris, France, Oct. 2014, pp. 5332–5336. doi: 10.1109/ICIP.2014.7026079.
[106] J. A. Kloess, J. Woodhams, H. Whittle, T. Grant, and C. E. Hamilton-Giachritsis, “The Challenges of Identifying and Classifying Child Sexual Abuse Material,” *Sex Abuse*, vol. 31, no. 2, pp. 173–196, Mar. 2019, doi: 10.1177/1079063217724768.
[107] A. Gangwar, E. Fidalgo, E. Alegre, and V. González-Castro, “Pornography and child sexual abuse detection in image and video: A comparative evaluation,” 2017.
[108] N. Sunde and I. M. Sunde, “Conceptualizing an AI-based Police Robot for Preventing Online Child Sexual Exploitation and Abuse:: Part I – The Theoretical and Technical Foundations for PrevBOT,” *NJSP*, vol. 8, no. 2, pp. 1–21, Jan. 2022, doi: 10.18261/issn.2703-7045-2021-02-01.
[109] Wikipedia contributors, “Sweetie (internet avatar) — Wikipedia, the free encyclopedia.” 2022. Accessed: Nov. 30, 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Sweetie_(internet_avatar)&oldid=1108753708
[110] Medietilsynet, “En kartlegging av 9-18-åringers digitale medievaner.” Medietilsynet, Oct. 2020. Accessed: Nov. 30, 2022. [Online]. Available: https://www.medietilsynet.no/globalassets/publikasjoner/barn-og-medier-undersokelser/2020/201015-barn-og-medier-2020-hovedrapport-med-engelsk-summary.pdf
[111] L. R. Frøyland, G. M. Solstad, P. L. Andersen, and S. B. Tveito, “Seksuelle overgrep mot barn og unge via digitale medier,” *NOVA Rapport*, p. 211, 2021.
[112] F. Mayer *et al.*, “Age estimation based on pictures and videos presumably showing child or youth pornography,” *Int J Legal Med*, vol. 128, no. 4, pp. 649–652, Jul. 2014, doi: 10.1007/s00414-014-1012-2.
[113] O. Cullen, K. Z. Ernst, N. Dawes, W. Binford, and G. Dimitropoulos, “‘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*, vol. 9, no. 4, p. 28, Nov. 2020, doi: 10.3390/laws9040028.
[114] T. W. Trøen, “Lovvedtak 165,” p. 2, Aug. 2021.
[115] C. Ongre, “Feedback from: Ministry of Local Government and Modernisation.” Apr. 08, 2021. Accessed: Nov. 30, 2022. [Online]. Available: https://ec.europa.eu/info/law/better-

regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665314_en
[116] M. R. Calo, "The Boundaries of Privacy Harm," *Indiana Law Journal*, vol. 86, no. 3, p. 31, Jul. 2010.
[117] D. K. Citron and D. J. Solove, "Privacy Harms." Boston University Law Review, Sep. 02, 2021. Accessed: Nov. 30, 2022. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222
[118] Y. E. Bigman and K. Gray, "People are averse to machines making moral decisions," *Cognition*, vol. 181, pp. 21–34, Dec. 2018, doi: 10.1016/j.cognition.2018.08.003.
[119] P. N. K. Schuetz, "Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for an Adaptive Legal Framework," *lawineq*, vol. 39, no. 1, pp. 221–254, 2021, doi: 10.24926/25730037.626.
[120] Europol, "The Internet Organised Crime Threat Assessment (IOCTA) 2017," 2017.
[121] V. A. Jensen, "Offentlig og privat satsning mot hvitvasking og terrorfinansiering (OPS AT)," *Bits AS*, Nov. 05, 2021. https://www.bits.no/offentlig-og-privat-satsning-mot-hvitvasking-og-terrorfinansiering-ops-at/ (accessed Nov. 30, 2022).
[122] Økokrim, "Enheten for finansiell etterretning (EFE) - Økokrim," *Økokrim*, 2022. https://www.okokrim.no/finansiell-etterretning-fiu.549302.no.html (accessed Nov. 30, 2022).
[123] Økokrim, "Årsrapport 2021 - Enheten for finansiell etterretning." 2021. Accessed: Jan. 06, 2022. [Online]. Available: https://www.okokrim.no/getfile.php/5020921.2528.ptpjjbqmjkpnbj/%C3%85rsrapport+2021.pdf
[124] United Nations, "Human Rights," *United Nations*, 2022. https://www.un.org/en/global-issues/human-rights (accessed Nov. 30, 2022).
[125] Council of Europe, "Lanzarote Convention," *Children's Rights*, 2022. https://www.coe.int/en/web/children/lanzarote-convention (accessed Nov. 30, 2022).
[126] Statista, User-generated internet content per minute 2022. Available from https://www.statista.com/statistics/195140/new-user-generated-content-uploaded-by-users-per-minute/ (accessed Dec. 20, 2022)
[127] Joleby, M., Lunde, C., Landström, S., & Jonsson, L. S. (2021). Offender strategies for engaging children in online sexual activity. *Child Abuse & Neglect*, *120*, 105214.
[128] Google Transparency report 2021, available from https://transparencyreport.google.com/child-sexual-abuse-material/reporting?lu=urls_deindexed&urls_deindexed=period:2021H2. Accessed Dec 20, 2022.
[129] Apple Fandom. NeuralHash, available from https://apple.fandom.com/wiki/NeuralHash. Accessed on Dec 20, 2022.

Acronyms

AI	Artificial Intelligence
AR	Augmented Reality
BIK+	European strategy for a better internett for children
BSI	Basic Subscriber Information
C3P	Canadian Centre for Child Protection
CAE	Child Abuse and Exploitation
CSA	Child Sexual Abuse
CSAM	Child Sexual Abuse Material
EFE	Unit for Financial Intelligence
EMPACT	European Multidisiplinary Platform Against Criminal Threats
ESP	Electronic Service Provider
ICMEC	International Centre for Missing and Exploited Children
ICSE	International Child Sexual Exploitation
ISP	Internet Service Provider
IWF	Internet Watch Foundation
MD5	Message-Digest Algorithm 5
MR	Mixed Reality
NCMEC	National Center for Missing and Exploited Children
NTNU	Norwegian University of Science and Technology
P2P	Peer-to-Peer
SARS-CoV-2	Coronaviruspandemic (Covid-19)
SHA	Secure Hash Algorithm
SOBI	Sexual abuse of children over the internett
STR	Suspicious Transaction Report
STRASAK	Norwegian criminal case register
TLD	Top-Level Domain
TOR	The Onion Router
UNICRI	Interregional Crime and Justice Research Institute
URL	Uniform Resource Locator
VoIP	Voice-over-IP
VPN	Virtual Private Network
VR	Virtual Reality
XR	Extended Reality

BI Norwegian Business School is a leading Nordic research and teaching institution with campuses in the four largest Norwegian cities. Our activity is organized under nine departments covering the range of business research disciplines, and eight BI Research Centres concentrated around themes where we are especially strong.

Departments

- Accounting and Operations Management
- Communication and Culture
- Data Science and Analytics
- Economics
- Finance
- Law and Governance
- Leadership and Organizational Behaviour
- Marketing
- Strategy and Entrepreneurship

BI Research Centres

- Centre for Asset Pricing Research
- Centre for Construction Industry
- Centre for Corporate Governance
- Centre for Creative Industries
- Centre for Experimental Studies and Research
- Centre for Health Care Management
- Centre for Applied Macroeconomics and Commodity Prices
- Nordic Centre for Internet and Society

For an archive of all our PhD-dissertations/reports, please visit https://www.bi.edu/research/publications/

SERIES OF RESEARCH REPORTS 01/2023
ISSN 0803-2610

BI Norwegian Business School

BI Norwegian Business School
N-0442 Oslo
Phone: +47 46 41 00 00
www.bi.no