




End(-to-end
encrypted)

**Child
Sexual
Abuse
Material**



CyberPeace | Foundation



Warning: This report contains content that may be
distressing for some readers. Reader discretion is advised

Title: End (-to-end Encrypted) Child Sexual Abuse Material

Copyright © 2020 Cyber Peace Foundation

L29-L34, First Floor, Connaught Place, New Delhi 110001, India

This report titled *End (-to-end encrypted) Child Sexual Abuse Material* has been developed by the Technology, Law and Policy research group of Cyber Peace Foundation (CPF). The research group developed technical tools solely for the purpose of this study. CPF reserves all rights to this publication. No part of this report may be used for sale/promotion, reproduced, replicated or redistributed without prior permission of CPF. For any queries regarding this report, please reach out to: secretariat@cyberpeace.net

About CPF:

CPF is a non-profit initiative that works to build collective resilience against cyber-attacks and crimes, promote a truly inclusive cyberspace and institutionalise global peace in a digital century. As the world's first organisation devoted to promoting cyber peace, CPF works with stakeholders across different verticals including technology companies, academia, law enforcement, government, civil society and end users to advocate for stronger institutions and frameworks that foster inclusive global development. For more: www.cyberpeace.org

Research and Writing:

Akshata Singh

Nitish Chandan

Raj Pagariya

Sachet Sahni

Shipra Sahu

Srushti Iyer

ISBN: 978-93-5416-448-4

Executive Summary

Until recently, the distribution arrangements for Child Sexual Abuse Material (CSAM) had been largely identified on the public web and the dark web. In these areas, the technology industry, regulators and policy makers have been making steady and measurable progress. However, of late, the focus of CSAM distribution has shifted to end-to-end encrypted (E2EE) services offering high levels of anonymity and negligible prosecution with an extremely low barrier to entry.

The research group undertook this study, between June 2020 to July 2020, to assess E2EE platforms as a new mode of CSAM distribution. The objective of this research was to specifically study and analyse technical, legal and policy frameworks that can help prevent proliferation of CSAM on E2EE communication services. Most countries/commentators have taken an either-or approach to propose solutions, where it is *either* monitoring of content *and* *invasion* of user privacy or *no regulation* and *free flow of objectionable content at alarming levels*. This report presents an objective assessment of effectiveness of reporting mechanisms on the platforms and identifies practical ways of tackling CSAM while balancing user privacy. In a dedicated section, the report proposes a model design and operationalisation strategy for reporting CSAM in an E2EE setting which does not violate user privacy. The researchers have also identified and highlighted the importance of other techno-legal and operational gaps and challenges associated with CSAM including initiatives like National Tip-Line, mandatory report CSAM buttons for intermediaries in India, National Hash Register etc.

The report exhaustively studies different E2EE services, while presenting primary findings from investigations into two platforms prevalent among Indian users : WhatsApp and Telegram. The selection of these platforms for our primary research was also based on features which facilitate wider dissemination of CSAM, such as chat invite links that enable users across the world to join a chat group on such platforms. The mode of data collection on the platforms was deployment of custom tools to gather data, and then in-depth analysis of content and reporting mechanisms. In the study, we found over 100 instances of dissemination of CSAM in just 29 randomly selected adult pornography groups on WhatsApp, while 23 such instances of dissemination from 283 channels analysed on Telegram. In due course of time, an addendum to this report in the form of a white paper for legislators will be published highlighting the need and extent of duty of care and liabilities of intermediaries in context of E2EE services and CSAM.

APPS IN FOCUS*

WhatsApp

1299

total adult
pornography
groups
identified

29

groups
studied in-
depth

over
100

instances
of CSAM

content found being shared through images,
videos, stickers.

0

out of 15 groups removed after
reporting through multiple
channels

4

out of 29 reported users
banned after sharing
screenshots of illegal use

Telegram

350

total adult
pornography
channels
identified

283

channels
studied in
depth

23

instances
of CSAM

171

channels removed after
reporting through multiple
channels

*Findings from End (-to-end Encrypted)
CSAM Report 2020

Contents

Executive Summary	3
1. Background	6
2. Online Modes of CSAM Proliferation	11
2.1. Surface Web.....	11
2.2. Peer-to-peer (P2P) file sharing platforms.....	12
2.3. Dark Web	15
2.4. End-to-End Encrypted Communication Services	16
3. Industry and Legislative Initiatives and Research	
Rationale	19
4. E2EE Communication Services.....	22
5. Apps in Focus: WhatsApp and Telegram.....	23
5.1. WhatsApp.....	23
5.2. Telegram	26
6. Gaps and Recommendations.....	29
6.1. Reporting Gaps	30
6.2. Gaps in Enforcement.....	33
Annexes.....	36
Annex A- CSAM Regulation and Policies from the World	36
Annex B- Review of E2EE services.....	47
References.....	49

1. Background

With the revolutionisation of worldwide communication by the internet in 1990s, online Child Sexual Abuse Material (CSAM) transmission gained momentum when established offline distribution and production channels were already fully functional. The advent of novel, complex, and advanced technology offered internet users unparalleled anonymity and efficiency, giving offenders the means to share and sell CSAM through such networks while creating newer challenges of enforcement and policy response in an inter-connected world.

On the subject of usage of terms ‘child pornography’ and CSAM, the definition and usage of both terms have evolved over time. The term child pornography, while ly embedded in several international conventions and domestic legislations, has been associated with visual content and has evolved in its legal and colloquial usage for over several decades. In 1989, the CRC defined ‘child pornography’ narrowly as ‘the exploitative use of children in pornographic performances’. However, as instances of depiction of sexual exploitation of children evolved from graphic images and videos to animated depiction and computer-generated content involving children in sexual activity, the definition for ‘child pornography’ also became broader. Accordingly, the Lanzarote Convention 2007 defined child pornography as ‘any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child’s sexual organs for primarily sexual purposes’ (Council of Europe, 2007). Due to its prevalent use in international legal instruments, child pornography remains a commonly used term in both international conventions and domestic legislation for defining creation and dissemination of child sexual exploitation material (CEM) (Greijer & Doek, 2016). However, the use of CSAM or child sexual exploitation material (CEM) is gaining ground among international agencies and child protection agencies to replace child pornography, in order to aptly capture the gravity of this offence.

According to the Terminology Guidelines endorsed by INTERPOL, the term CSAM can be used for material depicting acts of sexual abuse and/or focusing on the genitalia of the child while the term child sexual exploitation material can be used in a broader sense to encompass all other sexualized material depicting children (Greijer & Doek, 2016). Accordingly, with the exception of legal definitions, this report will use CSAM/CEM to address creation, distribution and possession of such content.

The Federal Bureau of Investigation (FBI) was the first agency to investigate online CEM/CSAM groups through its 'Operation Innocent Images' launched in 1994. During the investigation, FBI discovered an alarming trend of sexual exploitation of children via computer networks. The agency noted that there were shifting trends, at the time, from computer bulletin boards to chatrooms for sharing CSAM and grooming children for sexual contact and producing CSAM (FBI, n.d.). These trends have shifted wider now, with more technologically sophisticated modes of CSAM proliferation.

While the creation and transmission of CSAM is criminalized all over the world, the transnational nature of this offence poses a huge challenge for all law enforcement agencies. Specifically, it makes tracing the origin of CSAM, identification of victims, and offenders more difficult. Due to its manifold forms, CSAM covers a wide range of activities, including storing, circulating or capturing CSAM, grooming kids for sexual purposes, live streaming or recording CSAM for distribution, soliciting sexual favours from children, or coercing them to share sexually explicit images and videos. In 2006, when the International Centre for Missing and Exploited Children (ICMEC) published the first edition of its report on CSAM related laws across the world, only 27 countries had laws sufficient to combat CSAM while 96 countries had no specific legislation, in contrast to the ninth edition of its report in 2018, where 118 countries had sufficient legislation to combat CSAM while sixteen (16) countries across the globe did not have any legislation that explicitly addressed CSAM (ICMEC, 2018).

CSAM has been defined as the real or simulated depiction of : (a) overt sexual activities involving a child; or (b) private parts of a child, by means of videos, photos, drawings, cartoons, live streaming, and any other means of representation which could be transmitted (ICMEC, 2018). The lack of a universal legal definition of CSAM across multiple jurisdictions has led to vague and imprecise definitions causing uncertainty in conviction and ineffective penalties, which fail to avert creation and circulation of CSAM. Therefore, an international collaborative policy-based approach is required, inclusive of all stakeholders, which sets out the legal framework to assist intermediaries and law enforcement agencies in combatting CSAM by identifying CSAM related offences and responsibilities of platforms along with procedures for takedown of content, investigation powers, prosecution etc. Such an inclusive and collaborative approach could substantially reduce the online availability and proliferation of CSAM.

CSAM has emerged as a global threat after the impetus provided to it by the rapid technological advancement facilitating cheaper internet access, a massive

increase in number of smart phones users, a boom of social media, end to end encryption (E2EE) and cloud based services. Easy user access to online social media platforms and services has culminated into emboldened offenders to proliferate CSAM for both commercial gains and private use. Protection of children from such direct offline and online abuse along with distribution of CSAM, the effect of which causes re-victimisation is a basic human right that enables fulfilment of other human rights (Interpol, 2018). Articles 19 and 34 of the United Nations Convention on the Rights of the Child (UNCRC), declare sexual exploitation of children in any form to be a severe human rights violation. CSAM and other offences involving sexual violence against children such as human trafficking, incest, prostitution, sexual aggression make the mental and physical wellbeing of affected children a serious concern. However, despite several legislative frameworks across the world to enable fulfilment of the above-mentioned rights, there are glaring inadequacies in the regulatory sphere in ensuring child safety on online platforms.

Interestingly, in several domestic legal frameworks, the age of sexual consent is less than the minority age criteria for CSAM. While there is no international treaty for setting the minimum age of sexual activity, the laws on minimum age for consensual sex vary mainly between fourteen (14) to sixteen (16) years of age (Greijer & Doek, 2016). In the US, minors aged fifteen (15) years and above can legally consent to a sexual activity with an adult. However, irrespective of age of consent for sexual activity, CSAM is considered to be content that involves or depicts a minor. For example the U.S. Federal Law on Child Pornography bars creation, distribution, or possession of a visual record of such activity involving a minor, that is, any person under eighteen (18) years of age (Department of Justice, 2020). The reason for a lower age of valid consent for sexual activity is that it recognises the evolution of individual capacity to engage in sexual relationships. However, it differs from CSAM which involves abuse or exploitation for which there is no relevance of consent (Greijer & Doek, 2016).

Statistics

Markovich (2017) concluded that anonymity on the internet along with easy access has resulted in a belief that viewing, sharing, or collecting CSAM is harmless and victimless. It becomes important in such a backdrop to enforce CSAM related laws and generate awareness and deterrence against committing any associated acts. In 1984, National Center for Missing and Exploited Children (NCMEC) was set up in the United States with the mission to prevent sexual exploitation and victimisation of children. Over the past decades, NCMEC has been institutionalised as the US nodal agency for receiving CSAM tips from

individuals and service providers. In the natural course of events, even service providers with a larger user base in India mandatorily report only to NCMEC owing to their legal requirements. Last year, National Crime Records Bureau (NCRB) in India signed an MOU with NCMEC to receive these tips where the country of origin was found to be India (Thaver, 2020). As per latest information received by this research group, a total of 35753 CyberTipline reports from NCMEC have been shared with concerned States and Union Territories and 201 FIRs and 42 arrests have been made based on such tip-offs.

Though CSAM is an issue of global concern, India is positioned as one of the largest consumers and creators of CSAM. As per a recent NCMEC report that compiled CSAM incidents on the internet, India stands at the top of the list with over 19.87 lakh reports (11.7%). Pakistan and Bangladesh are at the second and the fourth position with 11.5 lakh (6.8%) and 5.5 lakh (3.3%) reports, respectively (Kannan, 2020). According to a report by the Canadian Centre for Child Protection (2016), 78.30% of CSAM images and videos assessed by them depicted children under twelve (12) years of age while 63.40% of those children were under eight (8) years of age. Out of the total CSAM content reviewed, 80.42% of victims were girls, while the rest were boys (Canadian Centre for Child Protection, 2016). As far as perpetrators are concerned, a 2013 NCMEC report found that 18% of CSAM is generated by parents/guardians, 25% by a neighbour or family member, and 18% of CSAM is generated through online enticement/grooming (NCMEC, 2013).

From the United Kingdom, the Internet Watch Foundation (IWF) reported that out of all the reports received by them, 43% of images showed sexual activity between an adult and a child, including rape or sexual torture (Markovich, 2017).

In another report, IWF also reported identification of over 57,000 URLs containing CSAM in a single year (childsafenet.org, n.d.). The IWF report also noted a decrease in CSAM in the UK, from 18% in 1996 to less than 0.2% in 2015. While analysing the efficiency of notice and takedown procedures, it has been observed that 38% of web pages containing CSAM are removed within 60 minutes and 59% are removed within 120 minutes of receipt of takedown notices (Walshe, 2016). A similar observation was made by the International Association of Internet Hotlines (INHOPE) which found that 93% of CSAM removed in Europe and 91% CSAM worldwide was removed from public access on the Internet within 72 hours (Walshe, 2016).

India has recently instituted a national cybercrime reporting portal, of which CSAM is an essential part but data from the platform on reporting, takedowns etc. has not been reported widely.

2. Online Modes of CSAM Proliferation

The WeProtect Global Alliance (WPGA) published a report in 2019 on global threat assessment of online child sexual abuse. In its risk assessment, the report identified online CSAM distribution framework under three (3) heads based on the search-ability of content by standard web search engines, namely (i) Surface Web or Public Internet which is readily available to the general public. ; (ii) Deep web, which is not indexed by standard search engines and requires knowledge of direct URLs, IP addresses, credentials etc. to access, (iii) Dark web. While the dark web is still an evolving space on the internet, it is largely understood as the space which requires specialised software in order to be accessed like VPN networks, browsers etc. This study examines some of these identified distribution frameworks while also presenting more hybrid arrangements with lower barriers to entry and minimal filtering and prosecution.

2.1. Surface Web

The modes of distribution and access to CSAM have rapidly evolved over the years. The surface web, however, remains the most visible and active contributor to CSAM distribution worldwide. Distribution on the surface web includes use of websites, social media and other public platforms for sharing CSAM. For example, in 2018, INTERPOL identified a website on the surface web distributing CSAM that gathered millions of views in just a month (WeProtect Global Alliance, 2018). Easy access to such websites has made this a convenient distribution arrangement for CSAM across the world. Similar websites and perpetrators have been prosecuted in India where they were also found to be in possession of exorbitant amounts of money as proceeds of CSAM distribution business through certain websites (Hindustan Times, 2016). To some extent, even adult pornography platforms on the surface web have also allowed uploading and hosting of CSAM content on their websites (McGhee, 2020).

Investigation into such offences and locating perpetrators on the surface web is less difficult compared to other modes of online distribution, owing to the architecture of public web. In this regard, technological solutions can actively monitor and detect CSAM on public platforms and enable law enforcement to investigate up-loaders and downloaders of CSAM content. However, integration

of advanced technologies, such as encryption, on the surface web, has made detection and prosecution harder due to added layers of anonymity. Such advancement has also paved the way for innovative forms of abuse which are hidden in plain sight, such as live streaming of child abuse *via* several apps running on the surface web.

Social media platforms also make up part of this publicly accessible space. As per NCMEC data (2019), 15.8 million tips out of the total 16.8 million tips were received from the Facebook group, while social media platforms such as Reddit, Smule, Discord, Twitter etc. constituted substantial majority of sources for the remaining tips (NCMEC, 2019). Most of these platforms usually promote a zero-tolerance policy against CSAM. While some enforce it through technology solutions, others use reporting features to enhance detection and prosecution. Given the public nature of content and its access, it becomes possible, to some extent, to leverage user reporting of CSAM on scale.

2.2. Peer-to-peer (P2P) file sharing platforms

The set-up of peer-to-peer (P2P) file sharing platforms is a decentralized network which enables its users or peers to upload files for sharing purposes and download files shared by other users. P2P file sharing platforms were introduced in the year 1999 through Napster, a protocol created by a student named Shawn Fanning for music sharing (Encyclopedia Britannica, 2019). Mega and LimeWire are popular P2P content sharing platforms which have been known sources of CSAM content as well. While platforms differ in their functioning and underlying technology, the essence of P2P file sharing lies in direct access to only parties with knowledge of the mode of access.

Mega

Mega is a cloud-based P2P file sharing platform founded by Kim Dotcom whose earlier business Megaupload was shut down, owing to criminal charges pursued by the US Department of Justice for copyright infringement and piracy (Himler, 2013). Mega operates in a manner similar to platforms like Dropbox, with the exception that file sharing on Mega is E2EE (MEGA, 2016). As a cloud-based platform providing E2EE P2P file sharing, Mega claims that it does not have access to the content on its platform, nor are there any mechanisms for content monitoring and moderation, which is bound to cause problems.

Accordingly, Mega has a track record of numerous reported instances¹ of CSAM transmission that have been highlighted in the news, and predictably numerous others that are going unnoticed.

While conducting the primary research, this group came across several instances of CSAM file sharing over Mega. Based on the available evidence, it is apparent that a lack of a properly publicised reporting and takedown policy, has made Mega and other encrypted P2P file sharing platforms an easy and largely unmonitored medium for CSAM presentation, distribution and possession

While conducting primary research, this group came also across several instances where files containing CSAM were being shared over Mega.

Limewire

LimeWire is another P2P network for file sharing². While it was initially launched in 2000, the large-scale distribution of pirated content over LimeWire caused losses worth billions of dollars to the music industry (McIntyre, 2018). Accordingly, LimeWire was closed down in 2010, owing to multiple lawsuits resulting in awards of millions of dollars and investigation by US federal agencies. However, in the context of the significant role played by P2P file sharing platforms as media for CSAM transmission, it would be instructive to highlight LimeWire. LimeWire's active enabling of the search criteria and default sharing, caused large-scale CSAM proliferation on its platform³. To add to this, content downloaded pursuant to CSAM related search criteria were not only hosted but also available to other users for downloading. However, despite

¹ According to a press release dated 28 January 2020 by the US Attorney Office, District of Kansas, a person named Aaron McDowell was arrested on account of issuing a death threat to the President of the United States, and was later also charged with possession, presentation and distribution of CSAM. McDowell's *modus operandi* for CSAM possession and distribution mainly involved Mega. Specifically, the investigation team found 2800 CSAM images uploaded on McDowell's Mega account which was also used to share CSAM content with other users (Department of Justice, 2020). The availability of CSAM and transmission of CSAM on such a huge scale went unreported for a long time and the only reason CSAM was uncovered on the Mega platform was owing to the threat made to the President and not the rapid distribution of CSAM. In an older incident of 2012, the US law enforcement authorities confirmed the unearthing of CSAM from Megaupload's servers (Sothesian, 2013).

² The LimeWire platform provided access to Gnutella, a network and search protocol specifically for file sharing, which also offered anonymity to its users (Ripeanu, Lamnitchi, & Foster, 2002).

³ LimeWire's search protocol enabled users to locate and access files uploaded on other LimeWire accounts. The most dangerous and distinguishing feature of LimeWire was its default settings that made all files downloaded by a user through LimeWire available for download to other users. This provided a broader public network for content distribution as compared to other P2P file sharing platforms such as Mega.

offering such a large P2P network, LimeWire did not put in place any policy or mechanism to review, monitor or moderate its traffic data for objectionable content.

In 2012, when the U.S. General Accounting Office (GAO) undertook research to determine the ease of finding CSAM on P2P file sharing platforms, P2P platforms such as LimeWire were found hosting readily available CSAM. On putting twelve (12) keywords in one search on LimeWire, the GAO identified 1286 CSAM related titles and file names. In another search, with an input of three (3) keywords, 149 images out of the 341 downloaded files contained CSAM, which is about 40% (Roberts, n.d.). This clearly shows availability of CSAM in abundance due to a lack of sufficient reporting and monitoring mechanisms on the platform⁴.

In 2016, the US Court of Appeals for the Fifth Circuit released its opinion in the case of *United States of America v Jason Daniel Scott*. In this case, Mr. Scott was charged under 18 U.S.C. § 2252 (a) (2) (A) & (5) (B), on one count of possessing child pornography and on three counts of receiving child pornography. The Court's opinion extensively discussed the contents of the Presentence Investigation Report, which revealed undisputed facts relating to the major role played by LimeWire in enabling Mr. Scott⁵.

In the context of LimeWire's default file sharing feature, the court further recounted evidence from the investigation, which confirmed that the default sharing feature allowed the offender to “*not only receive . . . but to ‘distribute’ child pornography*” (United States of America v Jason Daniel Scott, 2016).

In this context, even if the argument of such intermediaries regarding difficulty in content monitoring due to voluminous data traffic is conceded to, the lack of employment of readily available technology to enable filtering and content monitoring of searches and downloads containing CSAM related keywords,

⁴ In fact, the risk perpetuated by LimeWire for distributing CSAM was so high that the FBI and other federal agencies had developed the software ‘ShareazaLE’ for the sole purpose of identifying and tracking individuals who used LimeWire or other P2P file sharing modes to download and share CSAM. The software enabled the FBI to download illicit videos and images from shared folders on a computer suspected of using LimeWire to engage in the CSAM related traffic (Floyd, 2016).

⁵ The relevant extract from the report is set out: “an investigation into the use of a computer program called LimeWire determined that Scott’s computer ‘was actively downloading and possessing child pornography’. The agents were able to download three illicit videos from the ‘shared’ file folder on Scott’s computer associated with LimeWire, and a forensic examination of Scott’s computer confirmed that those videos were downloaded from the internet.” (United States of America v Jason Daniel Scott, 2016).

demonstrates outright complacency. Accordingly, the alarming level of CSAM proliferation on P2P file sharing platforms must be controlled through stricter intermediary regulation and reporting, discussed in Section 6 of this report.

2.3. Dark Web

The dark web represents those parts of the internet that need specialised software, knowledge of URLs and other access parameters. URLs for websites hosted on the dark web and their access frameworks differ from the usually accessed public internet (Mansfield-Devine, 2009). This part of the internet has been flagged by researchers from time to time for hosting CSAM and other illegal content.

The reason for such overwhelming presence of CSAM on the darkweb is the anonymity that certain dark web P2P network servers and specialised routing services provide. In some cases, open access websites distribute CSAM images while several other websites offer paid access to CSAM. The high entry barrier for the dark web requires specific technological know-how, however, perpetrators are availing similar levels of anonymity through specific types of hybrid services on the surface web as well. A common procedure adopted by perpetrators is to host the content on a P2P file hosting platform, and to share the access link with password, once the uploader receives payment from the requesting user. In addition to this, some images may be sent as samples before such transaction (Neverauskaite, 2015).

P2P platforms along with use of cryptocurrency ensure anonymity in CSAM related transactions at unprecedented levels and have further escalated the CSAM proliferation on the dark web, and made it difficult for the law enforcement agencies to filter relevant information through multiple layers of anonymity (O'Malley, 2018). Without a doubt, there have been success stories such as Freedom Hosting and Operation Onymous (a crackdown operation on illegal online marketplaces in the dark web coordinated by enforcement agencies from various jurisdictions including Europol and the FBI), the proliferation has remained largely unaffected (Bronskill, 2016). A recent and prominent success story, is a 2017 investigation by the U.S. Department of Justice which busted a hidden CSAM website titled 'Welcome to Video' by following a Bitcoin trail on the dark web (Newman, 2019).

Hence, while several success stories cast hope on the horizon, with the advancement in technology and connectivity, the need for collaboration between law enforcement agencies across borders, for anonymous tips, and knowledge-sharing on cybercrime investigation is growing steadily.

2.4. End-to-End Encrypted Communication Services

End-to-end encryption (E2EE) has garnered momentum for instant messaging services in the last few years, and in many cases become default for secure communication services. In an E2EE communication model, the service provider does not possess decryption keys to the content being shared through their servers. In other words, a sender's message can only be decrypted by the intended receiver. It is believed that E2EE is a safer solution as it decreases the number of parties who may interfere or decrypt the contents. Further, it aims to ensure that a third-party cannot eavesdrop on message contents while it is being transmitted. For retrieving the message contents, a third-party would need to contact either the sender or receiver directly. Some obvious advantages of using E2EE include maintaining confidentiality and integrity of content, and the users' right to privacy. Given that privacy is recognised as a fundamental right across multiple jurisdictions, E2EE protects free speech by shielding journalists, newspaper correspondents, persecuted activists, and dissidents. Well-known applications such as WhatsApp, iMessage, Telegram, and Signal have adopted E2EE for their instant messaging applications.

E2EE based communication services rely on asymmetric cryptography (also known as *public-key cryptography*) wherein every user holds a pair of keys, namely, public key and private key. While the public key can be shared without any restrictions to send secure communication, only the user has access to his private key to decrypt the same communication. Keys in a pair are mathematically related to each other in a manner that a message encrypted using the public key can only be decrypted using the corresponding private key from the user's key pair (Ermoshina et. al, 2016). For two given users A and B, B will encrypt his message using A's public key and send it to A. A will decrypt this message using his private key. Seemingly complex in terms of operationalising, most of the services make their algorithms publicly available to demonstrate trust, robustness and protection from any kind of third-party surveillance.

The problem arises when the use of E2EE platforms for organised crime, terrorist activities, and CSAM, makes it difficult for law enforcement agencies to trace or prevent such acts (Endeley, 2018). The security and privacy provided by such services is undoubtedly a huge contributing factor towards increasing the overall trust in the internet. However, there have been substantial number of news articles, reports, and white papers which have found specific instances of CSAM transmission on E2EE communication platforms such as WhatsApp and Telegram, pointing to either gaps in policy or enforcement thereof. With

large user bases of 2 billion and 400 million, respectively, CSAM proliferation on such popular messaging platforms cannot be underestimated (Banerjee, 2020). While the terms of service of such E2EE communication platforms explicitly prohibit using the platform for transmission of objectionable content such as CSAM transmission, the research outcomes present an altogether different story of enforcement of such policies.

In April 2020, the Kerala Police collected IP addresses of more than 150 persons who were involved in CSAM transmission over Telegram (Express News Service, 2020). While this is undoubtedly not the first time when the Kerala Police has dealt with CSAM, older news articles such as Abraham (2017) cover how CSAM groups have been busted on the platform. Back in 2018, Apple had removed Telegram from its App Store for a brief period, pursuant to numerous reports of inappropriate content being shared (Fingas, 2018). In this regard, an investigation report by CPF in 2019 elaborated how Telegram serves as a mode for CSAM transmission through channels and private accounts (Chandan, 2019).

In alignment with CPF's report, two Israel-based NGOs, Screen Savers and Netivei Reshet also published their findings on how third-party apps containing WhatsApp group invite links were used for demanding and distribution of CSAM. The report further highlighted the inadequacy of current measures taken by WhatsApp (Constine, 2018). Following these reports, WhatsApp removed more than 130,000 user accounts for clamping down on sharing of CSAM through their platform. Investigations conducted by CPF observed similar findings (Chandan, 2019a). Besides, WhatsApp also shared information about such accounts with NCMEC (India Today Tech, 2019). It must be noted here that no publicly available reports confirm the sharing of relevant data by WhatsApp with any Indian authority or agency.

Investigation and arrest by enforcement agencies for CSAM transmission over E2EE communication platforms are not uncommon. In October 2019, CBI's special unit called Online Child Sexual Abuse and Exploitation Prevention/Investigation (OSCAE) arrested seven (7) individuals after receiving information from the German Police (Pandey, 2020). Earlier this year, on reports by several members of a WhatsApp group, the Jaipur Police arrested a man in January 2020 for sharing a CSAM video on the concerned WhatsApp group (Sharma, 2020). Similarly, in May 2020, the Karaikudi Police arrested an individual for sharing CSAM through WhatsApp for the last six (6) months (Veerappan, 2020).

It cannot be ignored that CSAM proliferation over the internet has increased over the years, and the adoption of E2EE for communication services has only

contributed to its undesirable growth. There is a general consensus among researchers and the civil society (and the finding of this research group) that installing backdoors or breaking encryption is not the ideal solution, as content moderation at the service-provider level will be prone to abuse. This is why the responsibility and accountability should lie with service providers to create effective policies and reporting mechanisms to prevent sharing and distribution of CSAM. Section 6 of this report discusses possible measures that could be taken in this direction.

3. Industry and Legislative Initiatives and Research Rationale

In 2000, the European Parliament and the Council of the European Union issued a directive 2000/31/EC on ‘electronic commerce’ which made Internet Service Providers (ISPs) liable if they possessed knowledge of illegal activity on their networks (EUR-Lex, 2000). While the directive itself does not prescribe a specific notice and takedown procedure, several successful voluntary self-regulatory schemes for notice and takedown have been implemented in member countries including Germany and the United Kingdom. In the United States, companies are required to report CSAM to NCMEC, which has operated the CyberTipline reporting function since 1998. NCMEC records and actions reports of suspected child exploitation, including CSAM, and works with ISPs to establish good practice and ensure effective processes. Another report by UNICEF and the GSMA (a global alliance representing the interests of mobile operators and adjacent industry sectors worldwide) called on the service providers and internet companies to effect policies on a notice and takedown approach towards checking CSAM transmission.

A closer look at such an approach demonstrates its effectiveness on the surface web where content can be retrieved by third parties and analysed for removal. However, such approach will not be possible in the context of E2EE services, let alone effective, unless patent technological changes are made. Section 6 of this report lays down various prerequisites and the necessary groundwork for implementing standardised functions for reporting CSAM and record keeping of such CSAM for enforcement purposes.

Individual ISPs have also taken measures to enable automated filtering of CSAM. The tech industry and civil society have collaborated from time to time to build innovative tools that enable such filtering and ensure zero-tolerance against CSAM. Initiatives like the Content Safety API tool by Google aids both commercial and non-governmental organizations in reviewing objectionable content and identifying CSAM (Sawers,2018). This tool claims 700% enhanced detection as compared to a human moderator in the same time frame (Sawers,2018). Similar APIs are offered by some other organisations, for example, Safer, developed by THORN and being currently offered to businesses in the US quickly flags CSAM content (Daws, 2020). Additionally, Google

displays deterrence advertisements for CSAM related queries and search by users and highlights CSAM material as unlawful.

The most notable and widely used breakthrough in this field is the PhotoDNA, a service offered by Microsoft to enable detection of CSAM through comparing of hashes. These hash databases are built with known and reported CSAM from across the world. This enables any platform to proactively detect CSAM by comparing data against a credible source of previously identified CSAM. **In the sphere of E2EE services, it becomes clear that such technology is also not effective or possible.** Some limited adaptations of the technology, however, are prevalent. WhatsApp, for example, relies on such technology to detect CSAM in the public information on the platform, such as group icons etc. Through active use of such technology, WhatsApp was able to ban around 250,000 accounts every month for sharing CSAM.

The Civil Society has also contributed substantially in the fight against CSAM over the years. The most notable contributions by the civil society include the UNICEF Child Online Protection guidelines for industry which stressed on the importance of multi-stakeholder collaboration and the development of standard operating procedures to handle CSAM (UNICEF, 2015).

In June 2020, the Global Partnership to End Violence Against Children (EVAC), an international entity launched by the UN Secretary General, partnered with Technology Coalition, comprising of approximately eighteen (18) global tech companies such as Microsoft, Google, PayPal etc. to launch the initiative titled 'Project Protect' to ensure child safety against online violence. The plan calls for inter-sectoral technologies, inclusion of tactics by stakeholders such as law enforcement agencies, civil societies, hotlines, governments etc. to combat CSAM. As per the press release by EVAC, Project Protect will involve significant investments for innovation in technology towards CSAM detection and prevention (End Violence Against Children, 2020). Under this project, EVAC will be responsible to conduct independent research and the global coalition will serve as the source for tech industries to combat CSAM.

Recently, the Five Eyes, an intelligence alliance comprising the UK, USA, Canada, Australia and New Zealand in collaboration with six global tech firms including Facebook, Google, Microsoft, Roblox, Snap and Twitter have designed eleven (11) voluntary principles to combat CSAM, after discussions with prominent tech companies, industry experts and academicians. These principles delineate active measures to fight CSAM and safeguard the victims. The voluntary principles are designed to be feasible for implementation by all technology enterprises, irrespective of their size (Five Country Ministerial,

2020). **However, it is argued that the most concrete and actionable principles (removing known CSAM, detecting CSAM etc.) would work well only for services on the surface web and not E2EE communication services.**

It can be argued that such E2EE communication is private, between people who know each other but it has been found through earlier research reports (Chandan, 2019) (Constine, 2018) how features like **invite links** make public dissemination of CSAM possible on these E2EE platforms as well. Given the advantages of easy public access, potential of monetisation and high levels of anonymity, the threat posed by CSAM on E2EE communication services is comparable to the dark web. It becomes imperative, in this context and space, to enhance the understanding of the functioning of E2EE services and relevant gaps in policy-making and enforcement, for stakeholders across the board including industry, civil society, and the government .

We have also conducted a detailed legislative review of more than 55 countries across the globe for their laws on CSAM in context of encryption, accountability, reporting etc. Findings of the review (attached in Annex A) point to a conclusion that there is no comprehensive framework in place that proactively or reactively deals with CSAM on E2EE platforms. While laws on CSAM are well documented by organisations such as ICMEC and ECPAT through their yearly reports, tremendous gaps are prevalent in the sphere of E2EE services as they remain unregulated and outside the purview of other laws and regulation.

We have found that a substantial number of countries have chosen to regulate encryption-based services and implement a license-based regime, but there is not much literature available that talks about efficacy of such a regime in checking CSAM proliferation over the internet.

A detailed review of CSAM and encryption laws for the covered countries is set out in Annex A.

4. E2EE Communication Services

The table below summarises the most popular and widely used communication services based on their user base, whether E2EE is provided on personal and group chats, whether it is possible to access groups/channels through publicly available links and content reporting options. This table acts as the basis for selecting and exploring WhatsApp and Telegram in detail in the next chapter. (A detailed table is provided in Annexure B)

Service	Global User Base	E2EE in personal chats	E2EE in group/channel	Group/channel invites through link
Facebook Messenger	1.3 billion	Optional, needs to be enabled for specific chats	No	No
WhatsApp	2 billion	Yes	Yes	Yes
Viber	1.17 billion	Yes	Yes	Yes
iMessage	Statistics not available publicly, but there are 1.4 billion Apple devices in the market.	Yes	Yes	No
Telegram	400 million	Yes, only in secret chats	No	Yes
LINE	200 million	Yes	Yes	Yes
Signal	10 million	Yes	Yes	No
CoverMe	Data not available	Yes	Yes	No
Silence	Data not available	Yes	NA	NA
Wickr	Data not available	Yes	Yes	Yes
Dust	Data not available	Yes	Yes	No

5. Apps in Focus: WhatsApp and Telegram

As discussed in Section 3 of this report, there is an information gap on the extent of CSAM proliferation on E2EE based communication platforms. While literature and scholarship is available on the proliferation of CSAM on surface and even dark web, there is insufficient research on the scale and more importantly, problems on E2EE platforms. **In contrast to the anonymity offered by the dark web that comes from malicious actors and facilitators, the anonymity offered by E2EE services comes from legitimate service providers alongside more public access.** To achieve a level of zero- tolerance against CSAM on such legitimate platforms, it becomes important to understand whether CSAM proliferates on them and **whether there are gaps that can be filled without breaching user privacy.** Accordingly, the research team undertook an in-depth investigation for the purposes of : (i) collecting primary data regarding CSAM proliferation on two (2) online E2EE communication platforms; and (ii) determining the responsiveness of such platforms towards reporting of CSAM dissemination. This section summarises the results of such investigation conducted on WhatsApp and Telegram, the two communication platforms with the largest user base in India.

5.1. WhatsApp

Past investigations into the platform have revealed demand and promulgation of actual CSAM on WhatsApp Groups twice (Chandan, 2019a). For this report, another round of investigation was conducted while drawing on findings and reports made to the platform in 2019. In early June 2020, it was found that 110 out of the total 182 WhatsApp group links that were shared with the platform in 2019 were still active and operating. Many of these groups that were directly reported to the platform either comprised of adult pornography groups or had group icons that were pornographic. Almost all groups that had a clear CSAM group icon or description were removed while groups with obscene pictures and names like “sister’s rape”, “only rape”, “virgin sister’s rape” etc. remain active. On one account, however, a CSAM group which had already been reported during the previous investigation in 2019 was still actively distributing CSAM as of June 2020. The evident lack of effectiveness of the in-app reporting features was further buttressed when this group was removed after being flagged to the platform through channels outside the reporting feature on the

app. This triggered a more in-depth investigation into groups along with reporting mechanisms to action CSAM and offending users.

5.1.1. Data and Methodology

A technical tool was developed to identify and compile a list of publicly available links to join WhatsApp groups containing pornographic content. The tool further scraped data from different websites for such groups. The websites were selected after simple search engine seeks for keywords like ‘adult’, ‘pornography’ etc. A short list of 1299 groups along with their group icons was automatically scraped from the **surface web**. These groups comprised both groups that had clear sexual content (group icon or description) and groups that did not.

5.1.2. Preliminary Observations

- a. Out of the total 1299 groups for which data was collected, 215 groups were no longer active (old date of posting the invite links).
- b. Out of the remaining 1084 groups, 565 groups had obscene, pornographic and derogatory group names or group icons.
- c. It was found that there were several group names in languages and scripts other than English, including Hindi, Punjabi, Tamil, Spanish, Sinhala etc.
- d. There were several groups for distributing rape videos (named as such) and several that solicited sex work.
- e. Out of the total sample size, only three (3) groups had clear CSAM in the group icon.
- f. 39 other groups had normal-seeming pictures of children with obscene group names/descriptions.

Despite a few threads emerging out of the preliminary findings (including solicitation of sex work, live streaming of abuse, sharing of malicious application files), the investigation focused on CSAM and reporting through the rest of the course of the investigation. In order to do a more in-depth analysis, 29 groups were randomly selected from a large pool of 1084 adult pornography groups

Note: None of these 29 groups contained explicit CSAM in the group icon or description.

5.1.3. Findings

Out of the 29 groups that were joined, none specifically endorsed or specified CSAM availability in any publicly available information. Activity on these groups was then monitored for a period of eighteen (18) days. The findings from such investigation are set out below:

- a. There were irregular demands for CSAM on the groups through more colloquial references like *cp*, *kids videos* (in hindi) etc. These demands were not always met and were from both Indian and foreign phone numbers.
- b. Out of the total of 29 groups, CSAM was ultimately shared on fifteen (15) groups by 30 users. The volume and frequency at which CSAM was shared on each group was different. However, there were specific instances where the same content appeared on multiple groups. While there were no patterns to such content sharing, in several instances, CSAM videos appeared along with a bulk video upload, for example, out of 50 videos uploaded in one single go, 4-5 videos could be CSAM. Upon the upload of CSAM videos on such groups, there was an increase in user demand for CSAM. Overall, more than 100 CSAM videos were uploaded during the research period.
- c. An interesting finding was that there were quite a few self-produced videos of a child alone or two children engaged in sexual activity together.
- d. CSAM was also found being shared through the stickers feature of the app.
- e. There were over a dozen rape videos including gang rape, which had likely Indian victims (given language, dialects used in the videos)

5.1.4. Reporting

As part of mandatory reporting and responsible disclosure from the research group, continuous reporting of the content was carried out on the National Cyber Crime Reporting portal (www.cybercrime.gov.in). The WhatsApp platform offers two (2) modes of reporting, one from within the groups or chats and the other through the Help-Contact section from the app. The in-group reporting feature is a generic report function and does not provide a feature to classify the nature of content being reported. This is also due to the end-to-end encryption of group chats and the platform's technical limitation of viewing the content. The second reporting/contact section allows a user to upload a screenshot along with a question. These fifteen (15) identified groups were then reported via both these channels during the research period.

On reporting such content from within the app, it was found that none of the groups were removed and four(4) users that uploaded CSAM were banned or blocked, notwithstanding the specific knowledge regarding the precise nature of CSAM and knowledge of the instance of upload that was imparted to WhatsApp via screenshots on the app itself. Interestingly, in email responses from the platform, it was made clear that any user reporting should not provide screenshots of the actual CSAM because such communication would lead to transmission of CSAM over email, while providing no other channel to report the details of CSAM. This could lead to multiple technical and legal complications. However, this makes it clear that there is no process for the platform to acquire actual knowledge of CSAM with the platform outside of the in-chat report button. After this, the fifteen (15) groups were then reported to the platform via direct channels (without any CSAM content). While none of the groups were still removed, it was later reported to the research group that many offending users were banned. Out of the 30 users who uploaded CSAM on the groups, only one user was banned. 25 of the 29 users who were reported (along with screenshots of them having uploaded CSAM on a group) remain active on the date of issuance of this report. In all likelihood, the technical limitation to view E2EE content leads to failure in action against these groups despite the maximum possible escalation.

While there is no evidence to substantiate this fact, it is highly likely, given the wide user base of WhatsApp in India and many other countries, that many of these videos and pictures are not available on the surface web (to be detected or flagged initially) and in fact, proliferate through WhatsApp groups and messages only. Therefore, it becomes pertinent to at least reactively, action such content.

5.2. Telegram

The report by CPF in 2019 had previously demonstrated an instance of how CSAM proliferates on Telegram (Chandan, 2019b). For this report, a detailed investigation on similar lines was conducted for over six (6) weeks to examine the extent of CSAM proliferation on the platform and the *modus operandi* employed by the perpetrators.

5.2.1. Data and Methodology

From publicly available links of Telegram channels for pornographic content, a total of 283 channels were joined. *Prima facie*, none of these channels had any explicit mention of CSAM, CEM or child pornography. But the channel names and description contained words such as *young*, *teenagers*, *CP*, and *school girls*.

It must be noted here that Telegram channels are not E2EE and can be reported under different categories.

5.2.2. Preliminary Observations

After observing the content being shared on these channels for over a week, it became manifest that the perpetrators had devised a standard *modus operandi* for distribution of CSAM on Telegram, which enabled them to avoid detection which is exacerbated due to no in app reporting feature for individual accounts. This included solicitation on adult pornography groups by using names or other indicators to hint at the intention to distribute CSAM, subject to payments.

Our preliminary observations during the investigation were as follows:

- a. Initially, 350 publicly available links for Telegram channels were gathered. Out of these, nineteen (19) links did not exist, and 48 channels had already been deactivated for being misused to spread pornographic content.
- b. The remaining 283 channels had obscene and sexually explicit channel names, icons, and descriptions.
- c. Channel names were in English, Hindi, Tamil, Telugu, Spanish, and Russian.
- d. On these channels, the content could be easily classified into the following heads:
 - Solicitation of sex work;
 - Sexually explicit content involving adults, produced by a well-known production house;
 - Self-recorded videos;
 - Thumbnails of individuals appearing to be minors with links to other channels and users; and
 - Fictional sexually explicit content.

5.2.3. Findings

During the investigation, a total of 23 instances were encountered where users were proliferating CSAM. These instances also included fictional CSAM. Three (3) instances appeared to be based out of India. The standard *modus operandi* of the perpetrators as observed during the research is set out below:

- a. Soliciting demand for CSAM by sharing a blurred picture depicting a minor involved in a sexual act with the link to a user account or bot across a large number of Telegram channels.
- b. The user account/bot shares samples and payment details. The user account/bot would often have words like *VIP*, *Premium*, *CP*, etc. or emojis of young boys and girls in the username.
- c. Payment is generally accepted over PayPal, PhonePe, or in the form of cryptocurrency acceptable to the CSAM distributor.

5.2.4. Reporting

On Telegram, groups and channels can be reported across five categories: Spam, Violence, Child Abuse, Pornography, and Other. Telegram offers a secret conversation feature which is E2EE, neither user accounts nor any specific content shared by a user in a secret conversation can be reported.

In their FAQs, Telegram states: “*All Telegram chats and group chats are private amongst their participants. We do not process any requests related to them.*”.

While there is no mechanism to report the private user accounts, we reported all such channels that were involved in spreading pornography or child abuse. More than 85% of the channels reported from within the app have been removed as on the date of the issuance of this report. Alternatively, Telegram has also provided abuse@telegram.org email address for reporting illegal content on Telegram, but only for channels, bots, and sticker sets.

Even after a reporting mechanism is put in place, there is an explicit limitation at Telegram’s end in identifying CSAM due to E2EE private conversation between two users. Another important finding is associated with bias in the removal of channels reported under the category of *Pornography*. While channels with less than 100,000 followers were removed after a maximum of two (2) reports, certain reported channels with more than 200,000 followers continued to operate despite reporting such groups multiple times.

6. Gaps and Recommendations

There are several levels and fronts at which potential solutions to the proliferation of CSAM have been generally proposed. For one such level, countries aim to regulate content at the ISP level. This is proposed by monitoring, filtering and blocking access to websites known to be distributing CSAM (Office of the Regulator Samoa, 2016). This more passive way alongside other active detection technology, works well within a limited sphere of the public internet where content can actually be monitored and filtered. On another level, countries attempt to make intermediaries and ISPs liable for hosting CSAM on their networks. Such a model has not been fully operational in any jurisdiction yet, but it presents its own sets of merits and demerits.

The issue, however, that has been identified through this research is that most of the regulatory and industry attempts focus largely on the surface/public internet while not venturing into the grey pseudo-anonymous sphere of E2EE services. The Asia-Pacific Financial Coalition against Child Sexual Exploitation, for example, under its Technology Challenges Working Group, identifies best practices for file hosting and sharing services but does not go insofar as to talk about E2EE services (ICMEC, n.d.). One of the reasons for such exclusion of E2EE services in all previous regulatory attempts was made apparent through the recent US Government attempt to water down intermediary immunity, commonly known as safe harbour provisions, through the EARN IT Bill. Through the discourse, emerged an inherent threat to user privacy, security and free speech while trying to monitor or filter CSAM on E2EE services (Cope, Mackey, & Crocker, 2020). There have also been some technical proposals like client-side scanning of content for known CSAM (Pfefferkorn, 2020) but we concur with the Internet Society's opinion (Internet Society, 2020) to the extent that a blanket scanning of content will hamper user privacy. This report, however, goes further in asserting that the status quo of E2EE services needs to change without hampering user privacy which, in fact, is possible. As has also been highlighted in the previous chapters, features of bulk invitations and public invite links to join groups and channels that are E2EE have facilitated and enabled dissemination of CSAM. In light of such status quo of platforms (in facilitating widespread dissemination of adult pornographic content on groups), it becomes highly difficult to filter out any CSAM, rape videos etc.

One immediate step in this direction could be controlling the scope and availability of public group invite links. Platforms can design and deploy techniques to operationalise such control to the effect of preventing users from

easy and global access to groups that disseminate any type of objectionable content.

In the most recent governmental development in this area, an expert process as part of the EU Internet forum 2020 has been launched to identify technical and regulatory solutions to detect and report CSAM in an E2EE environment (European Commission, 2020). It also lays down a principle of balance between privacy of electronic communications and interventions against CSAM as critical to implementing any possible solution. To that extent, this report supports the European Commission's stance and principles, based on which a few recommendations and models have been proposed hereafter, with India in focus but having global applicability, nonetheless.

6.1. Reporting Gaps

In the attempts to achieve zero-tolerance against CSAM, huge emphasis has been laid on reporting, even in other contexts, like file sharing services (ICMEC, 2013), frameworks to takedown content where re-victimisation happens (UNICEF & GSMA, 2016) etc.

The set of eleven (11) voluntary principles recently signed by major companies have also highlighted the need for preventing previously identified CSAM from being made available on the platform, identification of new CSAM content and reporting, identifying grooming and other preparatory activities along with solicitation, recruitment and advertisements etc. (WeProtect Global Alliance, 2020). Despite the initiatives, these principles in operation remain unratified and without a clear strategy of operation on E2EE communication platforms. As has been identified in the earlier chapters, there is a clear lack of standard reporting mechanism. This is absent both in the cases of user-to-platform reporting and platform-to-government reporting (in India). Moreover, there is no model of accountability and liability, whatsoever, in cases of absence of the duty of care and wilful negligence by E2EE communication services, outside of governmental reporting. In simple terms, it means that there is no liability on a platform to act on CSAM, rape videos etc. upon receiving actual knowledge of such illegal content through user reports. In order to exhaustively and technologically analyse and present the issue of duty of care and liability to legislators and policymakers worldwide, this research group will also publish an addendum note to this report in due course of time.

6.1.1. Recommendations on Operationalising CSAM Reporting

In view of our findings above, we propose a model represented by Figure 1 below for reporting CSAM on E2EE communication service platforms without

violating user privacy (Proposed Reporting Mechanism). The Proposed Reporting Mechanism operates on the need for a regulatory/legislative action to mandate a report CSAM button on all platforms. Implementing this model for CSAM reporting will be the first major step by any country towards credible detection of CSAM and a zero-tolerance policy for CSAM on E2EE communication services. Currently, the only way such platforms manifest their intent to combat CSAM is by making a passing reference to dissemination of objectionable content as prohibited use under their terms of service. However, a mandatory report CSAM button, alongside providing the channel to streamline CSAM related traffic, also demonstrates a clear, unambiguous intention of all platforms to deter proliferation of CSAM through the platform. The Proposed Reporting Mechanism will comprise three stages, set out below:

Stage 1

At the time of reporting CSAM, the end user will have an option to tag the problematic content by way of a simple selection within the chat. This selected content (which is stored on the user's device in an unencrypted environment) is used to create a hash value. Then, this hash (not the actual content) is communicated to the platform for verification as per step 2a, thereby maintaining the platform's E2E integrity and ensuring that problematic content gets reported at the same time.

Stage 2a

Thereafter, depending on the national/international norm, the platform verifies that particular hash value with existing repository for CSAM content in hash registers like the PhotoDNA. Upon receiving a match confirmation, as per the nation's reporting requirements, the relevant authorities/regulators are notified for legal action against the uploader. This mechanism is particularly resilient in India's legal context where publishing, sharing, downloading etc. of CSAM outside of reporting is also considered a punishable offence and will go a long way in building the much needed deterrence against transmitting CSAM and preventing re-victimisation of victims. This also furthers the principle of removing/actioning known CSAM on platforms without violating any user privacy. The process of reporting ends here if a match is found with existing CSAM.

Stage 2b

In the second stage, if no hash value match is found in the first stage, the reporting user is notified. At this point, the user has an option to report the content as new CSAM (in line with the eleven (11) voluntary principles) with the

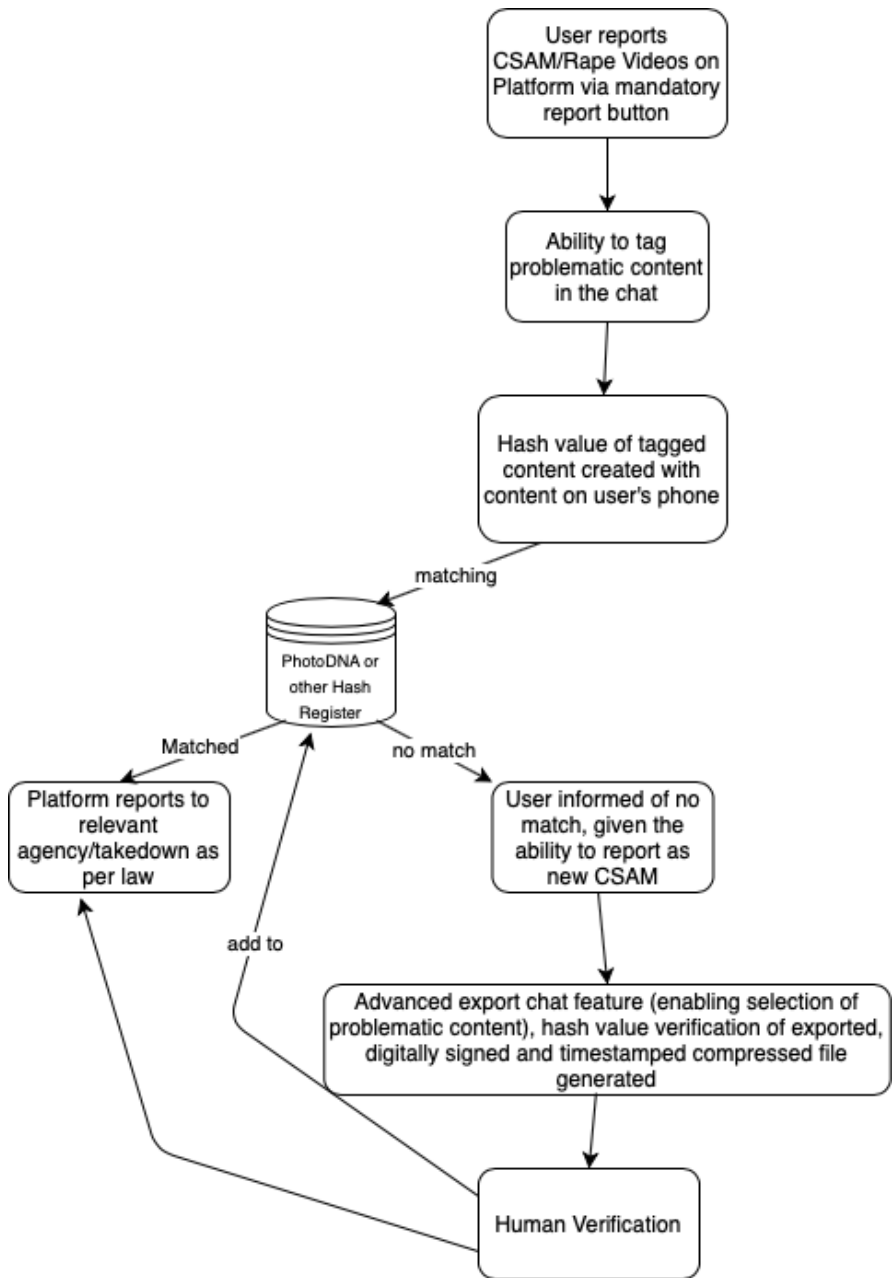


Figure 1 Model Reporting Process Design for E2EE services

use of an advanced chat export feature. This feature will enable the reporting user to tag the potential CSAM content within the chat and create a compressed chat file (similar to the WhatsApp chat export feature). Any platform will need to integrate significant product change to introduce this feature. The differences with a simple export chat feature being:

- a. such a compressed file will not comprise of the entire chat;
- b. only the content tagged by reporting user will be compressed so as to not make it a resource heavy exercise;
- c. the resultant compressed file is digitally signed or provides an automated notice of authenticity or such logging mechanism that does not increase the overhead on a platform's system; and
- d. the platform automatically stores an md5 or other file verification hash value of the resultant compressed file which can be later requisitioned by law enforcement for forensic verification, if required.

The platform will further enable uploading of this compressed file by the user. Content from such user report and the compressed file will be vetted preferably through human review, either directly or after one round of automated analysis using machine learning techniques like detection of nudity in a graphic, frames in a video etc.

Stage 3

After conclusively verifying presence of CSAM in the reported content, the same reporting mandate to the authorities/regulator as set out in Stage 2a will be followed in such cases, alongside addition of this new content as a hash value into the existing hash register like PhotoDNA. In case the content in question is found to be non-CSAM, the user will be notified, and if the user is not satisfied with the response, she can file a complaint with the relevant regulator. The process of reporting for new CSAM ends here.

Note: It is important that the boundaries of the intermediary liability are clearly defined within the bracket of identifying and notifying new content and existing content received through these reports. Intermediaries should not be made liable for active monitoring of content because such moderation defeats the purpose of E2EE and user privacy.

6.2. Gaps in Enforcement

While the Ministry of Home Affairs in India has streamlined the reporting of online transmission of CSAM and rape videos through the cybercrime.gov.in

portal (National Cybercrime Reporting Portal) pursuant to directions of the Supreme Court (*In re: Prajwala*, 2018). However, through the course of this research, we have identified patent problems and gaps in the reporting mechanism on the government portal that are set out below:

- a. Reporting on the National Cybercrime Reporting Portal can only be done after the complainant selects a jurisdiction, down to the district and police station level. It is safe to assume that this approach is not adequately equipped to address complaints against cybercrimes given their borderless nature. Needless to say, for people who report such crimes, this process can be utterly confusing and redundant.
- b. Real enforcement action viz. arrests and convictions in such offences, may require co-operation amongst agencies in multiple jurisdictions which becomes difficult and complicated when a local agency undertakes an investigation.
- c. As on the date of issuance of this report, a user can either report anonymously or through a report and track option on the National Cybercrime Reporting Portal. In the report and track feature (when user would want to be contacted/aware of the developments in the complaint and investigation), it is mandatory to upload a valid national ID of the victim (irrespective of the complainant) without which a report cannot be made. This hampers any scope of reporting by whistleblowing users who are willing to report CSAM that they encounter on E2EE platforms but do not know the identity or whereabouts of the victim.

6.2.1. Recommendations

- a. **Standard Operating Procedure:** A national Standard Operating Procedure (SOP) on last mile reporting and handling of content at police stations needs to be built and communicated that mandates law enforcement officers to deal with sensitive content. This has to be provisioned by reporting clauses for law enforcement and uploading mechanisms. This will help build on a national hash register that will enable effective removal of content.
- b. **National Hash Register:** Either by way of participation in the PhotoDNA model (which is the practice as of today) or setting up another hash register, India needs to lay solid groundwork for a national hash register. This hash register for CSAM/Rape videos must also be made accessible to members of the civil society so as to enable them to report content that they might come across in the course of their work relating to CSAM.

- c. **Regulatory and Legal Changes:** The **mandatory report CSAM** button and a **user-to-platform and platform-to-regulator** reporting channel **discussed** as part of the **Proposed Reporting Mechanism**, needs to be implemented by way of a legislative change or a regulatory policy.
- d. **National Online Safety Regulator:** As part of the proposed policy changes in order to consolidate efforts to tackle CSAM, either a new national online safety regulator should be set up or a special wing should be carved out from within the existing framework of NCRB, CBI etc. Within the regulator/enforcement agency, a model for accountability and speedy disposal of complaints needs to be set up with a follow up mechanism with the agency that ultimately handles the complaint on the ground.
- e. **National Tip-line:** With the draft Information Technology (Intermediaries Amendment) Rules, 2018 still in the pipeline, it is unclear whether intermediaries operating with a wide user base in India will be required to incorporate a separate entity under Indian law. Regardless, as per a strong reporting paradigm, a national tip-line like the CyberTipline maintained by NCMEC in the US is needed urgently. Though the National Cybercrime Reporting Portal plays a vital role in this ecosystem, yet, given the jurisdictional and procedural issues discussed in Section 6.3, it is not sufficient for tracking and nabbing CSAM perpetrators. Accordingly, a national tip-line needs to be operationalised to serve the following purposes:
- focal point for mandatory reporting requirements as per Section 19 of the POCSO Act (although the Cybercrime Portal does that, it does not cover intermediaries at this point);
 - focal point for reporting by intermediaries (also E2EE communication services in this context);
 - management of the national hash register including, coordination with relevant agencies for updating and other maintenance activities associated with the register; and
 - coordination with NGOs and other members of the civil society to deploy hash register technology for enhanced last mile reporting.

Annexes

Annex A- CSAM Regulation and Policies from the World

International and Regional Conventions

At the international level, there are various legal instruments that deal with CSAM and CEM. The most significant conventions include the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography of 2000 (OPSC) and the European Convention on Cybercrime of 2001. Article 19 in the Convention on the Rights of the Child places an obligation on the governments to take adequate measures to protect children from any sort of abuse or exploitation (ICMEC, 2017).

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (also known as Lanzarote Convention 2007) prescribes the nations to take necessary steps to safeguard the victims of CSAM and provide with efficient investigation and prosecution mechanisms to identify the perpetrators. Similarly, the African Charter on the Rights and Welfare of the Child requires states to protect children from any kind of abuse or sexual exploitation under Article 27. Further, it mandates the governments in African countries to take measures to prevent children from coercion or inducement to indulge in any form of sexual activity. In addition, the African Union Convention on Cyber Security and Personal Data Protection (also known as the Malabo Convention 2014) seems to address the CSAM issue at the regional level. It includes a definition for CSAM under Article 1, followed by an obligation on the states under Article 29(3)(2) to take requisite legislative actions (Salian & Khatun, 2020).

Africa

South Africa has criminalised CSAM through the Films and Publications Act, 1996 and the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007. Section 18(1)(c)(ii) of the latter deals with online grooming while Section 19 defines ‘child pornography’ and its scope. Encryption-based services are majorly governed by the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 along with the Electronic Communications and Transactions Act, 2002. Section 21 of the former law provides for decryption mechanisms for providing assistance to law enforcement agencies after receiving an order from the court. Section 29 of the

former mandatorily requires encryption-based service providers to get their service registered (Comninos, 2012).

Ethiopia has neither signed nor ratified the Optional Protocol. Further, its law is limited to display of simulated sexual intercourse by a child and exhibiting a child's genitals. With this limited scope, the federal law does not cover a wide range of exploitative acts that can be committed against children leading to the production of CSAM (ECPAT International, 2007a). While there is no direct legislation dealing with encryption, Ethiopia criminalises manufacturing or assembling of any telecommunication service without prior permission.

Section 333 bis 1 (new) of **Algeria's** Penal Code defines and criminalises 'child pornography'. This provision is comprehensive enough to cover virtual CSAM (ECPAT Global Database, n.d.). Though Algeria is not a signatory to the Council of Europe Convention on Cybercrime, it complies with OPSC norms and strictly prohibits CSAM. On the other hand, Article 3 of Law 09-04 of August 2009 lists down rules to prevent crimes related to ICTs and allows for search and seizure of computer systems (Algerian Chamber of Commerce and Industry, n.d.). Article 5 of the same law can be interpreted to empower authorities to decrypt data using external support.

In **Morocco**, it is illegal to own and distribute pornographic material of any kind. Article 503 of the Morocco's Criminal Code prohibits sale, possession, distribution, production, import, export, etc. of CSAM and provides for criminal sanctions (CRIS, 2014). While Morocco has ratified the Optional Protocol, it is not clear whether Article 503 covers virtual CSAM or not. Article 13 of Law 53-05 on the Electronic Exchange of Legal Data requires prior registration/licensing of encryption-based services. Supplying, importing, or exporting an encrypted service without prior authorisation is a punishable offence. Article 33 of the same legislation talks about penalty when a criminal offence is committed using an encryption-based service.

Tunisia does not have any law that specifically deals with CSAM. Article 232 of the Penal Code remotely deals with prostitution of minors. The **Egyptian** law bans circulation, publication, and exhibition of audio, prints, and artistic items that are objectionable to public morality and decency. Further, preparing, assisting, facilitating, coercing, or threatening a child to practice acts which are against societal values is criminalised. However, there is no specific law dealing with exploitation of children on online platforms (ECPAT International, 2008). Similarly, there is no encryption-specific law. However, Article 64, Law Number 10 of 2003 on Telecommunication Regulation requires service operators to get a license before providing their services. It has been interpreted to mean that

this requirement is also applicable to encryption-based equipment and services.

Nigeria has existing laws that aim to combat commercial sexual abuse and exploitation of children such as the Child Right Act (CRA) and the Trafficking in Persons (Prohibition) Law Enforcement and Administration Act (TIP) (ECPAT International, 2007b). In 2019, a bill titled ‘the Internet Child Pornography Prevention Bill’ was proposed that states that ISPs registered or licensed by the Nigerian Communications Commission should not allow usage of its services, irrespective of the medium, to send, view, or retrieve content which involves child sexual abuse or exploitation. Contravention of the provision leads to hefty fines and makes the directors of service providers directly liable. The main objective of this bill is to discourage and prohibit the dissemination of CSAM through internet-based platforms.

Gambia has affirmed its commitment against child sexual exploitation at multiple forums. As per the Children’s Act of 2005, child prostitution is strictly prohibited. However, the law seems to be silent on online grooming of children and does not criminalise access or possession of CSAM (ECPAT International, 2015). On the other hand, **Benin** adopted the Child Code in 2015 that provides for a comprehensive framework for protection of children from commercial sexual exploitation and abuse. This code prohibits CSAM and prescribes penalties for exploitation of children for any type of sexual form against any form of consideration or remuneration (ECPAT International, 2017).

Botswana’s Children’s Act of 2009 provides for protection of children from exploitation, pornography, and prostitution. This act further mandates reporting and failure to report such exploitation is an offence. While there is no legal obligation on ISPs to report CSAM to law enforcement agencies, the 2009 Act criminalises possession as well as exposing children to pornographic material or using them to create pornographic content (ECPAT International, 2017).

Madagascar’s Penal Code was modified to include the definition of ‘child pornography’ in line with the requirements of the OPSC. Further, Article 22 of the Cybercrime Law prohibits dissemination of CSAM through digital means and prohibits recording, reproduction, or obtaining any sexually explicit material involving a child (ECPAT International, n.d.).

Sudan is a signatory to the Convention on the Rights of the Child as well as the OPSC. While there is no direct legislation dealing with CSAM, Section 235 of the Criminal Code talks about obscene material and the Informatics Offences (Combating) Act talks about content offensive to public morals. Neither of these

act specifically mention CSAM or child pornography. On the contrary, **Uganda's** Penal Code criminalises publication, advertisement, and possession of obscene material. Further, the Computer Misuse Act of 2011 bans possession, procurement, production, and distribution of CSAM. Uganda has a legislation called the Regulation of Interception of Communications Act for regulating communication surveillance and other related security services (Rokundo, 2016).

Australia and New Zealand

Australia has legislations to combat CSAM at federal as well as state levels. The 1995 Criminal Code categorises various offences relating to distribution, production, and accessing material that sexualises children. In Section 472.22 of the Code, the term 'internet' includes the Internet, mobile phones, and other electronic or wired devices. This provision along with § 471.19 and § 471.20 criminalise accessing, transmitting, soliciting, promoting, or causing CSAM over the internet, poster service, or any similar service (Bartle, 2020). In the case of *McEven v. Simmons* (2008), the New South Wales Supreme Court upheld a conviction in the case where the accused accessed cartoons from the Simpsons characters engaging in sexual interactions. This widens the ambit of CSAM to include fictional characters (NSW Law Reports, 2008).

For encryption, the Telecommunications Act of 1997 governs the obligation of ISPs to assist law enforcement and security authorities upon receiving requests or notices from the government or authorised agencies. Recently, the Australian Parliament passed the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill, 2018. This bill has now become an act and it allows law enforcement agencies to force businesses to hand over encrypted information and data (Newman, 2018). If a business does not have the power to intercept encrypted data, they will be asked to create tools to allow law enforcement or government to have access (Bocetta, 2019).

In **New Zealand**, § 3(2)(a) of the Films, Videos, and Publications Classification Act of 1993 deems a publication to be objectionable if it supports or promotes or tends to support or promote the exploitation of children (or younger persons) for sexual purposes. Possession of such objectionable content is punishable by an imprisonment up to ten (10) years or a fine up to \$50,000 (Netsafe, 2017). Law enforcement agencies, through the powers granted under the Search and Surveillance Act of 2012, can search and seize encrypted data and computers. The powers include compelling users to give up their passwords as well as encryption keys. Besides, companies can be asked to provide reasonable assistance to allow a law enforcement agency to gain access

to encrypted data. Similarly, as per the provisions of the Telecommunications (Interception Capability and Security) Act of 2013, network operators and service providers are duty bound to offer reasonable assistance to intercept and collect communications (University of Waikato, 2019).

Asia

India published a draft National Encryption Policy in 2015 that gave exclusive powers to the government to sanction cryptographic algorithms, regulating encryption-based services, and requiring prior licensing for commercial use of encryption (Mathur, 2015). This policy was never implemented owing to huge public outcry. § 67B of the Information Technology Act, 2000 criminalises publishing, transmitting, creating, collecting, seeking, browsing, downloading, promoting, advertising, exchanging, or distributing material in any electronic form depicting children in obscene, indecent, or sexually explicit manner. It also covers online grooming and facilitating the abuse of children online along with recording sexually explicit acts with children. This provision is further supported by §§14, 15, and 19 of the Protection of Children Against Sexual Offences Act, 2012 (POCSO Act). Under § 69 of the Information Technology Act, 2000 (IT Act), the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009 has been promulgated. Further, the recent changes proposed in the existing regulatory framework, evidence a shift in the legislative policy to tighten the grip around intermediaries such as WhatsApp. In December 2018, the Ministry of Electronics and Information Technology released the draft Information Technology (Intermediaries Guidelines (Amendment)) Rules, 2018 which proposed further intensification of the due diligence obligations imposed on intermediaries by requiring them to : (i) employ automated tools to filter out ‘unlawful’ content; and (ii) incorporate an entity in India, and have a 24x7 nodal officer to coordinate with enforcement agencies, if such intermediary has a user base of more than 5 million users. Additionally, the Rajya Sabha Adhoc Committee submitted its report in January 2020, regarding means to contain access and transmission of child pornography content on the social media. The Committee noted the prevalence of CSAM on social media and made 40 recommendations as an integrated package of measures (PIB, 2020), including recommendations for greater liability for intermediaries under the: (i) POCSO Act, by prescribing a Code of Conduct for intermediaries for maintaining child safety online, ensuring age appropriate content and curbing use of children for pornographic purposes; and (ii) IT Act to mandate proactive identification and removal of CSAM, reporting CSAM to Indian authorities and IP addresses/ identities of all those searching/accessing child porn/CSAM key words to

designated authority in India. While the recommendations of the Rajya Sabha committee are welcome measures, their implementation which requires large-scale amendments to existing statutes, is yet to be seen.

Further, to combat CSAM proliferation in India, in November 2019, the CBI has set up a special unit to collect information regarding online child sexual abuse. This unit is called as OCSAE (Online Child Sexual Abuse and Exploitation) Prevention/Investigation Unit and it has jurisdiction throughout the country for investigating such offences (Singh, 2019).

China has strict laws against pornography while there are no specific references to CSAM. Under Section 9, Chapter VI of its Criminal Law, heavy penalty is prescribed for any person involved in producing, reproducing, publishing, selling, or disseminating obscene material (Zhang, 2007). Unlike the mainland China, Hong Kong passed the Prevention of Child Pornography Ordinance on December 19, 2003 which criminalises possession, publication, and dissemination of CSAM (Hong Kong e-Legislation, 2003). China has enacted a strict licensing regime for E2EE services through its State Council Directive 273 of 2000 (Regulation of Commercial Encryption Codes). It designates the National Commission on Encryption Code Regulations (NCERC) as the chief regulator for commercial encryption. Any service provider, application, or business, that utilises encryption is required to apply for mandatory license before they commence their operations (AsianLII, 2020). On January 1, 2020, China's new Encryption Law came into effect. It retains the earlier approach of controlling the encrypted services through certification system prescribed by the government (Xinhua, 2019). On similar lines, the Chinese Counter-terrorism law sets out a legal obligation for providing the government with technical support, including backdoor access and decryption, to prevent and investigate terrorist activities (Zhou, 2016). E2EE platforms such as WhatsApp, Telegram, and Signal are banned in China.

Myanmar, through § 66(f) of the Child Law criminalises using a child in pornographic material. § 292 of Myanmar's Penal Code, 1860 criminalise several actions related to obscene materials such as sale, possession, distribution, public exhibition, etc. However, there are glaring inadequacies such as lack of criminal liability for downloading and accessing CSAM online and mandatory reporting requirements (Myanmar Centre for Responsible Business, 2017). § 69 of the Telecommunications Law penalises unauthorised disclosure of encrypted information with an imprisonment of one year and fine, it also provides scope for decryption requests under a court order (James, 2019).

Bahrain, under Article 10 of its Law on Combating Cyber Crimes, criminalises production and obtainment of pornographic material online. It specifically covers CSAM and lays down the penalty for ‘child pornography’. In a rare departure from the general trend of legislations across the globe, Article 9 criminalises using encryption to commit an offence such as the transmission of CSAM over the internet. The legislation provides several powers to for decryption and data disclosure. Article 13 allows the public prosecution to order any person, including any service provider, to transmit any information, covering data stored within an IT system or any information in its possession or control (ICMEC, 2019).

Israel has an array of offences that cover child sexual abuse. § 214b of the Israeli Penal Law criminalises possession, publication, and advertisement of obscene material involving a minor. § 368A goes on to prescribe punishment for such minor’s guardian, if the guardian consented to the commission of offence (Haaretz Editorial, 2018). Israel regulates encryption within its territory through three laws: Law Governing the Control of Commodities and Services Law, 1957, the Order Regarding the Engagement with Encryption Items, 1974, and the Commercial Encryption Items Export Controls Policy. Israel regulates encryption services through a licensing regime for use, development, production, import, and export of such services. For getting a license, a government assessment is mandatory, except for electronic signatures and open-source encryption. Israeli law also provides for a ‘Free Means License’ for certain technologies and applications that can be exempted from the licensing regimes. Under the Protection of Privacy Law, 1981 and the protection of Privacy Regulations, 2017, a database is required to be registered with the Registrar of Databases (Levush, 2016).

Through the Act on Regulation and Punishment of Acts Relating to Child Prostitution and Child Pornography and the Protection of Children, 1999, **Japan** has criminalised the production, possession, and provision of CSAM, including its storage on electronic records for distribution or personal use (Okuyama, 2006). However, there are no mandatory reporting requirements which cover social media platforms or E2EE services. A law enforcement agency may seek decryption of encrypted information if they obtain a court order to such effect (Umeda, 2016).

Americas

Argentina’s Article 128 of Penal Code makes it an offence to be involved in the production, distribution, publication, and representation of children under eighteen (18) years engaged in sexual activities (Giay, Fernandez, & O’Farrell,

2017). The Data Retention law requires businesses to intercept and forward the intercepted communication to authorities, when required by a court order. In 2009, the Supreme Court held the country's encryption law as unconstitutional and since then, there is no specific regulation dealing with encryption (EFF, n.d.).

Caribbean countries like **Antigua & Barbuda**, **Barbados**, **Jamaica**, and **Trinidad & Tobago** along with **Bahamas**, **El Salvador**, and **Ecuador** have criminalised possession, procurement, distribution, and production of CSAM (Peterson, 2013). Each of these countries have defined some sort of procedure under which a Magistrate or a judge or a police officer can seek decryption of encrypted data. Such provisions are supported by relevant punishments in case a person fails to comply with the Magistrate's order or a police officer's request (Global Partners Digital, n.d.).

Brazil's Child and Adolescent Statute, through Article 240, criminalises any individual involved in production and recording CSAM. Subsequently, Article 241A makes it punishable for anyone involved in the distribution and dissemination of such material through any means (Soares, 2008). Previously, there have been two court decisions in Brazil that have suspended the use of an encrypted communication app on the basis that those apps failed to comply with the court orders demanding contents of encrypted communications (Aleixo, et al., 2019).

§ 163.1(1)(a) of **Canada's** Criminal Code defines CSAM as nude or semi-nude sexual pictures or videos of a children under eighteen (18) years engaging in a sexual act. This provision also covers audio recordings, written statements, along with fictional CSAM. A maximum sentence of fourteen (14) years is prescribed. Besides, §§ 171.1. and 172.1 deal with making sexually explicit material available to a child and luring a child, respectively (Canada Justice Laws, 2020). Currently, there is no legislative power that can be used to require service providers to facilitate the decryption of encrypted information. However, depending on the technical infrastructure, certain case assistance orders or production orders can be passed under § 487 of the Criminal Code (Global Partners Digital, n.d.).

Article 366(D) of **Chile's** Penal Code criminalises the production of pornographic material involving children under eighteen (18) years of age. As far as encryption is concerned, there does not exist any specific regulation (Reuters, 2019). In **Columbia**, Article 218 of the Penal Code criminalises filming, possession, and transmission of children involved in sexual activity with an imprisonment of up to twenty years along with a fine of 150 to 1,550

current minimum wages (ICMEC, 2017). Just like Chile, there is no specific law on encryption, however, service providers are bound to offer encryption-based services to high government and intelligence officials (Global Partners Digital, n.d.).

There is no specific law regarding decryption of encrypted information in **Honduras**. Article 149D of the Honduras Penal Code criminalises distribution, production, and commercialisation of pornographic material involving children (US Department of Labor, 2013). On similar lines, Article 184A of **Peru's** Penal Code criminalises publication, distribution, and creation of pornographic material involving children (ICMEC, 2017). Just like Honduras, Peru does not have any regulatory limitation or restriction on E2EE services (Global Partners Digital, n.d.).

Article 175 of **Nicaragua's** Penal Code, Article 140 of **Paraguay's** Penal Code, Article 194 of the Penal Code of **Guatemala**, Article 231D of **Panama's** Criminal and Judicial Code, Article 312 of **Cuba's** Criminal Code, Article 173 of **Costa Rica's** Penal Code, Article 281 of the Penal Code of **Bolivia**, Article 1 of Law 17.815 of **Uruguay**, Article 351 of **Guyana's** Criminal Law Offences Act, Section 12 of the Electronic Crimes Act of **Grenada**, Article 24 of Law Number 53-07 against High-tech Crimes and Malpractice of the **Dominican Republic**, Article 48 of Law against Organised Crime and Terrorism Financing along with Article 24 of Special Law against Cyber Crime of **Venezuela**, and Article 200 of **Mexico's** Federal Penal Code prescribe punishment for persons involved in distribution, production, dissemination, and commercialisation of child pornography. However, none of these thirteen (13) countries have any specific law on encryption technologies (Global Partners Digital, n.d.).

In the **United States of America**, § 2256 of Title 18 defines 'child pornography' as any visual depiction of sexually explicit conduct involving a minor. Visual depiction includes videos, photos, digital, or computer-generated images. In the US, the federal-level laws explicitly prohibit the reception, possession, distribution, and production of CSAM through any means. Further, § 2251 criminalises persuading, enticing, inducing, or coercing a minor to engage or involve in a sexually explicit act. Besides, § 2251A prohibits a legal guardian or parent or any other person in custody of a minor to transfer custody, buy, or sell for the purpose of child pornography. First conviction under § 2251 of Title 18 of the United States Code leads to a minimum imprisonment of fifteen (15) years (Department of Justice, 2020). As of now, there is no legislative power that can be used to direct service providers to decrypt encrypted data. § 103(b) (3) of the Communications Assistance for Law Enforcement Act of 1994 specifies that telecommunication carriers cannot be required to decrypt, or

ensure that the government is able to decrypt, any communication that is encrypted by the customer, unless the encryption is provided by the carrier and they are able to decrypt it (Senseney, 1998).

Europe

At the EU level, there is a Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography of 2011 (EUR-Lex, 2011). Under Article 2(c), this directive presents a wide definition of ‘child pornography’ to include:

- a. visual depiction of a child engaged in either real or simulated sexually explicit conduct;
- b. any depiction of a child’s sexual organs for primarily sexual purpose;
- c. visual depiction of a person appearing to be a child engaged in either real or simulated sexually explicit conduct or any depiction of a person appearing to be a child’s sexual organs for primarily sexual purpose;
- d. realistic images of a child engaged in a sexually explicit conduct or realistic images of a child’s sexual organs for primarily sexual purpose.

While the EU classifies CSAM under the category of illegal conduct online, it promotes self-regulation initiatives. In the EU, the **United Kingdom** is the only country that has a standing legislation dealing with content moderation specific to E2EE platforms. Under § 253 of the Investigatory Powers Act, 2016, a technical capability notice can be issued to any operator to impose any applicable obligations on the operators to be able to provide assistance for interception or obtaining communications data or equipment interference authorised under the Act (Hern, 2017). § 90 of the Regulation of Investigatory Powers Act, 2000 contains powers for law enforcement agencies with regard to ‘protected information’ that is, electronic data that cannot be readily accessed or put into intelligible form. The earlier referred technical capability notice can only be issued when the Secretary of State is informed about the circulation of CSAM and there exists no way to moderate the content, though CSAM distribution, possession, and production is criminalised in the UK through the Sexual Offences Act, 2003 (Crown Prosecution Service, 2020).

Unlike many other countries across the globe, **Austria’s** law allows children who are fourteen (14) years and above to consent to make such content but only for personal use. Article 208(a) of the Austrian Penal Code prescribes a punishment of up to 5 years for production and distribution while mere possession attracts an imprisonment of up to two (2) years (Europol, 2005).

France has several laws related to encryption and encryption-base services. Article 30(1) of Law number 2004-375 provides that using the means of cryptology is free. Further, Article 871-1 of the Internal Security Code specifies that decryption means must be provided within 72 hours in case a reasonable situation exists or there is a requirement to investigate CSAM (Schulman & Bankston, 2017).

While **Spain** does not have any encryption-related laws, but it has ratified the Lanzarote Convention 2007 and Articles 127 bis, 177 bis, 179, 180 to 189 deal with prohibition of CSAM and subsequent punishments for various acts (ICMEC, 2018). Similarly, **Hungary** does not have encryption-related laws but it criminalises acts related to CSAM.

Germany's Ordinance of Implementation of Telecommunications Surveillance Measures states that if an entity encodes any information, they must ensure that they are capable of decrypting it. However, it appears that the ordinance is not applicable to E2EE. To solve this problem, Germany has been working on enabling a backdoor to allow the government to moderate content since last year (Leetaru, 2019).

Subsections (1) and (6) of § 97 of Law of Electronic Communications (2005) in the **Czech Republic** requires that all communication networks have to compulsorily install interfaces at specific points along the network to allow tapping and recording of messages. Further, if a service provider enables encryption, they must be able to ensure that it can be decrypted. However, the statutory law does not contain any provision related to encryption and it can be implied that the country's law does not cover E2EE as of now (CLFR, 2017). Distribution and production of CSAM in Czech Republic is criminalised and it is punishable with an imprisonment up to eight (8) years (Asiedu, 2007).

Article 12 of **Russia's** Federal Law number 128FZ (2007) mandates service providers to obtain license prior to operate E2EE service in Russia. One of the requirements service providers need to comply with is to give access to encrypted messages in case of suspicion or reasonable requirements. Several articles of Federal Law number 124FZ ascertain rights of children in the Russian Federation and criminalise the sale and distribution of CSAM (Huntley, 2013).

Annex B- Review of E2EE services

Service	Content Reporting Options	Public News Reports about CSAM	Part of any Coalition
Facebook Messenger	Messages in a secret conversation can be reported if they violate Facebook's Community Standards. Content related to bullying, sexual violence, or sexual exploitation constitutes a violation of the said policy.	Available	Facebook Group is a member of WeProtect Global Alliance.
WhatsApp	WhatsApp Terms of Service mentions illegal and obscene conduct; however, it does not specify child pornography or CSAM. A contact or group can be reported in its entirety, and a particular piece of content cannot be selected.	Available	Facebook Group is a member of WeProtect Global Alliance
Viber	Viber prohibits content that seeks to exploit or harm children by exposing them to inappropriate content.	Available	Could not be determined.

iMessage	Apple does not have any specific reporting feature for CSAM, though it does have a feature for reporting junk and spam.	News reports about Apple intercepting CSAM content based on hashes are available. This information is subsequently shared with NCMEC.	Apple is a member of WeProtect Global Alliance.
Telegram	Yes, child abuse is one of the categories under which content on a channel can be reported. However, there is no reporting feature to report individual user accounts.	Available	Could not be determined.
Signal	Signal does not mention any reporting policy in their terms and privacy policy.	Available	Could not be determined.
CoverMe	No reporting option for users.	Not available	Could not be determined.
Wickr	Nothing as such, for users.	Available	Could not be determined.
Dust	Reporting option available.	Available	Could not be determined.

References

- Abraham, B. (2017, December 26). *Kerala Police Bust Child Pornography Group On Telegram. Its Operations Will Sent A Chill Down Your Spine*. India Times: <https://www.indiatimes.com/news/india/kerala-police-bust-child-pornography-group-on-telegram-its-operations-will-sent-a-chill-down-your-spine-336231.html>
- Aleixo, G., Gobbato, A., Souza, I. D., Langenegger, N., Lemos, R., & Steibel, F. (2019, May 30). *The Encryption Debate in Brazil*. Carnegie Endowment for International Peace: <https://carnegieendowment.org/2019/05/30/encryption-debate-in-brazil-pub-79219>
- Algerian Chamber of Commerce and Industry. (n.d.). *ICT Regulations*. Algerian Chamber of Commerce and Industry: <https://www.caci.dz/en-us/Nos%20Services/Information%20Juridique/Pages/R%C3%A9glementation-TIC.aspx>
- AsianLII. (2020). *Regulation of Commercial Encryption Codes*. AisanLII: <http://www.asianlii.org/cn/legis/cen/laws/rocec383/>
- Asiedu, D. (2007, June 13). *Lower house approves amendment making possession of child pornography a crime*. Radio Prague International: <https://english.radio.cz/lower-house-approves-amendment-making-possession-child-pornography-a-crime-8468865>
- Banerjee, P. (2020, April 27). *Telegram now has 400 million users worldwide*. LiveMint: <https://www.livemint.com/companies/news/telegram-now-has-400-million-users-worldwide-11587972913622.html>
- Bartle, J. (2020, February 18). *Australia: Books, cartoons and dolls can amount to child pornography*. Mondaq: <https://www.mondaq.com/australia/crime/895042/books-cartoons-and-dolls-can-amount-to-child-pornography>
- Bocetta, S. (2019, February 14). *Australia's New Anti-Encryption Law Is Unprecedented and Undermines Global Privacy*. FEE: <https://fee.org/articles/australia-s-unprecedented-encryption-law-is-a-threat-to-global-privacy/>
- Broadhurst, R. (2019). Child sex abuse images and exploitation material. In *Handbook of Cybercrime* (pp. 310-336). Routledge.
- Bronskill, J. (2016, July 04). *Canadian police lack resources to keep up with online child pornography, federal memo warns*. The Star: <https://www.thestar.com/news/canada/2016/07/04/canadian-police-lack-resources-to-keep-up-with-online-child-pornography-federal-memo-warns.html>
- Canada Justice Laws. (2020, August 06). *Definition of child pornography*. Canada Justice Laws website: <https://laws-lois.justice.gc.ca/eng/acts/c-46/section-163.1.html>

- Canadian Centre for Child Protection. (2016, January). *Child Sexual Abuse Images on the Internet - A Cybertip.ca Analysis*. cybertip.ca: <http://s3.documentcloud.org/documents/2699673/Cybertip-ca-CSAResearchReport-2016-En.pdf>
- Chandan, N. (2019). *Second Report on Child Sexual Abuse Material and Chat Groups*. Ranchi, Jharkhand: Cyber Peace Foundation.
- Chandan, N. (2019). *Third Report on Investigation Into Child Sexual Abuse Material and Chat Groups*. Ranchi, Jharkhand: Cyber Peace Foundation.
- childsafenet.org. (n.d.). *Online Child Sexual Exploitation*. Child Safe Net: <https://www.childsafenet.org/online-sexual-abuse-exploitation>
- CLFR. (2017, May). *Provision of Real-time Lawful Interception Assistance*. Global Network Initiative: <https://clfr.globalnetworkinitiative.org/country/czech-republic/>
- Comninos, A. (2012). *Intermediary Liability in South Africa*. Association for Progressive Communications.
- Cope, S., Mackey, A., & Crocker, A. (2020, March). The EARN IT Act Violates the Constitution. *Electronic Frontier Foundation*.
- Constine, J. (2018, December 21). *WhatsApp has an encrypted child abuse problem*. TechCrunch: <https://techcrunch.com/2018/12/20/whatsapp-pornography/>
- Council of Europe. (1998). *Sexual exploitation, pornography, and prostitution of, and trafficking in, children and young adults (Recommendation No. R (91) 11) and report of the European Committee on Crime Problems*.
- Council of Europe. (2007). *Details of Treaty No. 201: Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*. Council of Europe: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201>
- CRIS. (2014, July). *Access to Justice for Children: Morocco*. Child Rights International Network: https://archive.crin.org/sites/default/files/morocco_access_to_justice_0.pdf
- Crown Prosecution Service. (2020, June 30). *Indecent and Prohibited Images of Children*. Crown Prosecution Service: <https://www.cps.gov.uk/legal-guidance/indecent-and-prohibited-images-children>
- Daws, R. (2020, July 31). AI tool detects child abuse images with 99% accuracy. *AINEWS*.
- Department of Justice. (2020). *Child Porn Charges Added To Threat Charge Against Salina Man*. Kansas: United States Department of Justice.

- Department of Justice. (2020, May 28). *Child Pornography*. The United States Department of Justice: <https://www.justice.gov/criminal-ceos/child-pornography>
- Department of Justice. (2020, May 28). *CITIZEN'S GUIDE TO U.S. FEDERAL LAW ON CHILD PORNOGRAPHY*. The United States Department of Justice: <https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography>
- ECPAT Global Database. (n.d.). *Algeria*. ECPAT Global Database: <https://globaldatabase.ecpat.org/country/algeria/#2.1>
- ECPAT International. (2007). *Global Monitoring Report on the status of action against commercial sexual exploitation of children: Ethiopia*. ECPAT: https://www.ecpat.org/wp-content/uploads/2016/04/Global_Monitoring_Report-ETHIOPIA.pdf
- ECPAT International. (2007). *Global Monitoring Report on the status of action against commercial sexual exploitation of children*. ECPAT International: https://www.ecpat.org/wp-content/uploads/legacy/Global_Monitoring_Report-NIGERIA.pdf
- ECPAT International. (2008). *Global Monitoring Report on the status of action against commercial sexual exploitation of children: Egypt*. ECPAT International: https://www.ecpat.org/wp-content/uploads/2016/04/Global_Monitoring_Report-EGYPT.pdf
- ECPAT International. (2015). *Global Monitoring Report on status of action against commercial sexual exploitation of children: The Gambia*. ECPAT International: https://www.ecpat.org/wp-content/uploads/2016/04/A4A_V2__AF_GAMBIA_FINAL2.pdf
- ECPAT International. (2017, March 30). *Submission for the Universal Periodic Review of the human rights situation in Benin*. ECPAT International: <https://www.ecpat.org/wp-content/uploads/2017/09/2017-%e2%80%93Benin-UPR-Report-Eng.pdf>
- ECPAT International. (2017, June 28). *Submission on Child Sexual Exploitation in Botswana for the Universal Periodic Review of the human rights situation in Botswana*. ECPAT International: <https://www.ecpat.org/wp-content/uploads/2018/07/Universal-Periodical-Review-on-Sexual-Exploitation-of-Children-Botswana.pdf>
- ECPAT International. (n.d.). *Madagascar*. ECPAT International: <https://globaldatabase.ecpat.org/country/madagascar/#1>
- EFF. (n.d.). *Mandatory Data Retention: Argentina*. EFF: <https://www.eff.org/issues/mandatory-data-retention/argentina>

- Encyclopedia Britannica. (2019, April 03). *Napster*. Retrieved June 23, 2020, from Encyclopedia Britannica: <https://www.britannica.com/topic/Napster>
- End Violence Against Children. (2020, June 11). *Project Protect: A New Initiative to End Violence Online*. End Violence Against Children: <https://www.end-violence.org/articles/project-protect-new-initiative-end-violence-online>.
- Endeley, R. (2018). End-to-End Encryption in Messaging Services and National Security - Case of WhatsApp Messenger. *Journal of Information Security*, 95-99.
- Ermoshina, K., Musiani, F., & Halpin, H. (2016). End-to-End Encrypted Messaging Protocols. *Third International Conference, INSCI 2016 - Internet Science* (pp. 244-254). Florence, Italy: HAL.
- EUR-Lex. (2000). *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')*. EUR-Lex: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031>
- EUR-Lex. (2011, December 11). *Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA*. EUR-Lex: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02011L0093-20111217>
- European Commission. (2020). *EU strategy for a more effective fight against child sexual abuse. Psikologi Perkembangan*. Brussels. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf
- European Financial Coalition Against Commercial Sexual Exploitation of Children Online. (2015, February 24). *Commercial Sexual Exploitation of Children Online*. Europol: <https://www.europol.europa.eu/publications-documents/commercial-sexual-exploitation-of-children-online>
- Europol. (2005). *Child Pornography: Legislation within the European Union*. genovaweb.org: http://www.genovaweb.org/materiali/minori/Legislation_on_Child_Pornography_Public1.pdf
- Express News Service. (2020, April 17). *Kerala cops collect IP addresses of 150 people who downloaded child porn amid lockdown*. The New Indian Express: [newindianexpress.com/states/kerala/2020/apr/17/kerala-cops-collect-ip-addresses-of-150-people-who-downloaded-child-porn-amid-lockdown-2131516.html](https://www.newindianexpress.com/states/kerala/2020/apr/17/kerala-cops-collect-ip-addresses-of-150-people-who-downloaded-child-porn-amid-lockdown-2131516.html)
- FBI. (n.d.). *Operation Innocent Images*. FBI: <https://www.fbi.gov/history/famous-cases/operation-innocent-images>

- Fingas, J. (2018, February 05). *Apple briefly pulled Telegram over child pornography distribution*. engadget: <https://www.engadget.com/2018-02-05-apple-briefly-pulled-telegram-over-child-porn-distribution.html>
- Five Country Ministerial. (2020). *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse*. The New York Times: <https://int.nyt.com/data/documenthelper/6803-11-voluntary-csam-principles/19d90625d84b3362a326/optimized/full.pdf>
- Floyd, J. (2016, July 13). *Sentence for Distribution of Child Porn Vacated by Fifth Circuit*. John T. Floyd Law Firm: <https://www.johntfloyd.com/sentence-enhancement-distribution-child-porn>.
- Giay, G., Fernandez, D., & O'Farrell, I. (2017, May 09). *Argentina: Draft Bill Makes Possession Of Child Pornography A Crime*. Mondaq: mondaq.com/argentina/crime/592584/draft-bill-makes-possession-of-child-pornography-a-crime
- Global Partners Digital. (n.d.). *World map of encryption laws and policies*. Global Partners Digital: <https://www.gp-digital.org/world-map-of-encryption/>
- Greijer, S., & Doek, J. (2016). *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*. Luxembourg: ECPAT International.
- Haaretz Editorial. (2018, December 05). *A Pornographic Bill*. Haaretz: <https://www.haaretz.com/opinion/editorial/a-pornographic-bill-1.6719759>
- Healy, M. (2004, August 02). *Child pornography: an international perspective*. Computer Crime Research Center: <http://www.crime-research.org/articles/536/>
- Hern, A. (2017, March 29). *UK government can force encryption removal, but fears losing, experts say*. The Guardian: <https://www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act>
- Himler, P. (2013, January 20). *Kim Dotcom Reaps Mega PR*. Forbes: <https://www.forbes.com/sites/peterhimler/2013/01/20/mega-pr/#152b14df2949>
- Hindustan Times. (2016, July 26). *Couple arrested for allegedly operating child porn websites in Chennai*. Hindustan Times: <https://www.hindustantimes.com/india-news/couple-arrested-for-allegedly-operating-child-porn-websites-in-chennai/story-hUEJcQJahVp83jv28PTYP.html>
- Hong Kong e-Legislation. (2003). *Prevention of Child Pornography Ordinance*. Hong Kong e-Legislation: <https://www.elegislation.gov.hk/hk/cap579>
- Huntley, S. (2013, April). *Russian Legislation on the Protection of Children Against Sexual Abuse and Sexual Exploitation: A Review*. ICMEC: https://www.icmec.org/wp-content/uploads/2015/10/Russian_Legislation_on_Protection_of_Children_Against_Sexual_Abuse_and_Exploitation_FINAL.pdf

- ICMEC. (n.d.). APFC Technology Challenges Working Group. <https://www.icmec.org/APAC-Tech-Challenges/>
- ICMEC. (2013). *Confronting New Challenges in the Fight Against Child Pornography :Best Practices to Help File Hosting and File Sharing Companies Fight the Distribution of Child Sexual Exploitation Content*. ICMEC: [icmec.org/confronting-new-challenges-file-hosting-and-file-sharing/](https://www.icmec.org/confronting-new-challenges-file-hosting-and-file-sharing/)
- ICMEC. (2017, April). *International Legal Instruments*. ICMEC: <https://www.icmec.org/wp-content/uploads/2017/04/International-Legal-Instruments.pdf>
- ICMEC. (2017, October). *National Child Protection Legislation: Colombia*. ICMEC: <https://www.icmec.org/wp-content/uploads/2017/10/ICMEC-Colombia-National-Legislation.pdf>
- ICMEC. (2017, August). *National Child Protection Legislation: Peru*. ICMEC: <https://www.icmec.org/wp-content/uploads/2017/08/ICMEC-Peru-National-Legislation.pdf>
- ICMEC. (2018, December). *Child Sexual Abuse Material: Model Legislation & Global Review (Ninth Edition)*. ICMEC: <https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf>
- ICMEC. (2018, November). *National Child Protection Legislation: Spain*. ICMEC: <https://www.icmec.org/wp-content/uploads/2018/11/ICMEC-Spain-National-Legislation.pdf>
- ICMEC. (2019, April). *National Child Protection Legislation: Bahrain*. ICMEC: <https://www.icmec.org/wp-content/uploads/2019/04/ICMEC-Bahrain-National-Legislation.pdf>
- India Today Tech. (2019, January 09). *WhatsApp has blocked 1,30,000 accounts in 10 days to fight child pornography*. India Today: <https://www.indiatoday.in/technology/news/story/whatsapp-has-blocked-1-30-000-accounts-in-10-days-to-fight-child-pornography-1427114-2019-01-09>
- Internet Watch Foundation. (2015, March 10). *Emerging Patterns and Trends Report #1: Online-Produced Sexual Content*. Internet Watch Foundation: https://www.iwf.org.uk/sites/default/files/inline-files/Online-produced_sexual_content_report_100315.pdf
- Internet Watch Foundation. (2018, May). *Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse*. IWF: <https://www.iwf.org.uk/sites/default/files/inline-files/Distribution%20of%20Captures%20of%20Live-streamed%20Child%20Sexual%20Abuse%20FINAL.pdf>

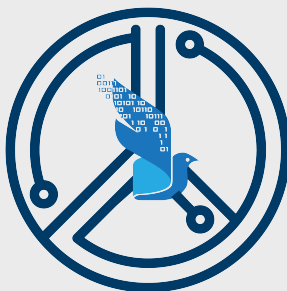
- Interpol. (1995). *Interpol recommendations on offences against minors*. Interpol 61st General Assembly.
- Interpol. (2018, March). *Towards a global indicator on unidentified victims in child sexual exploitation material*. ECPAT: <https://www.ecpat.org/wp-content/uploads/2018/03/TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL-Summary-Report.pdf>
- James, K. (2019, May 09). *Digital rights under growing pressure in Myanmar*. DW Akademie: <https://www.dw.com/en/digital-rights-under-growing-pressure-in-myanmar/a-48356715>
- Kannan, R. (2020, April 18). *Most online content on child sexual abuse from India*. The Hindu: <https://www.thehindu.com/news/national/most-online-content-on-child-sexual-abuse-from-india/article31377784.ece>
- Levush, R. (2016, May). *Government Access to Encrypted Communications: Israel*. Library of Congress: <https://www.loc.gov/law/help/encrypted-communications/israel.ph>
- Mansfield-Devine, S. (2009). Darknets. *Computer Fraud & Security*, 4-6.
- Markovich, E. (2017). *Two Clicks Away - An analysis of the offence of viewing child sexual abuse materials on the Internet (Master Thesis)*. Lund, Sweden: Faculty of Law, Lund University.
- Mathur, N. (2015, September 22). *What was the draft encryption policy and why it was withdrawn?* LiveMint: <https://www.livemint.com/Politics/RZtAGhM6ljDBWujik6ysEP/What-was-the-encryption-policy-and-why-it-was-withdrawn.html>
- McGhee, K. (2020, March). Pornhub has been caught hosting rape and child pornography. Don't fall for its coronavirus publicity stunt. *Washington Examiner*. Washington Examiner: <https://www.washingtonexaminer.com/opinion/pornhub-has-been-caught-hosting-rape-and-child-pornography-dont-fall-for-its-coronavirus-publicity-stunt>
- McIntyre, H. (2018, March 21). *The Piracy Sites that nearly Destroyed the Music Industry*. Forbes: <https://www.forbes.com/sites/hughmcintyre/2018/03/21/what-happened-to-the-piracy-sites-that-nearly-destroyed-the-music-industry-limewire/#a85f84032d7e>
- MEGA. (2016). Security and Privacy. <https://help.mega.nz/webclient/security-and-privacy.html#how-does-the-encryption-work>
- Myanmar Centre for Responsible Business. (2017). *Children's Rights and Business in Myanmar*. Yangon, Myanmar: Myanmar Centre for Responsible Business.

- National Center for Missing and Exploited Children. (2019). 2019 Reports by Electronic Service Providers (ESP). <https://www.missingkids.org/content/dam/missingkids/gethelp/2019-reports-by-esp.pdf>
- Netsafe. (2017, April 04). *Child Sexual Abuse Material and NZ Law*. Netsafe: <https://www.netsafe.org.nz/csam-law/>
- Neverauskaite, J. (2015, June). *In the Shadows of the Internet: Child Sexual Abuse Material in the Darknets*. ECPAT: <http://ecpat.be/wp-content/uploads/2015/03/Analyse-6-CSAM-in-the-Darknets.pdf>
- Newman, L. (2018, July 12). *Australia's Encryption-Busting Law Could Impact Global Privacy*. Wired: <https://www.wired.com/story/australia-encryption-law-global-impact/>
- Newman, L. (2019, October 10). *How a Bitcoin Trail Led to a Massive Dark Web Child-Porn Site Takedown*. Wired: <https://www.wired.com/story/dark-web-welcome-to-video-takedown-bitcoin/>
- NSW Law Reports. (2008, December 08). *McEwen v Simmons and Another*. NSW Law Reports: <https://nswlr.com.au/view/73-NSWLR-10>
- Office of the Regulator Samoa. (2016). *A filtering system to prevent access to Child Sexual Abuse Material on the Internet*. Office of the Regulator Samoa: regulator.gov.ws/images/Policies/Policy---Filtering-System-for-CSAM-APPROVED.pdf
- Okuyama, M. (2006). Child Abuse in Japan: Current problems and future perspectives. *JMAJ*, 370-374.
- O'Malley, R. (2018, June). *Commercial Child Sexual Abuse Markets on the Dark Web*. Criminal Investigations and Network Analysis: <https://cina.gmu.edu/publications/commercial-child-sexual-abuse-markets-on-the-dark-web/>
- Owen, G., & Savage, N. (2015). The Tor Dark Net. *Global Commission on Internet Governance - Paper Series: No. 20*.
- Pandey, D. (2020, June 03). *Child pornography: CBI books Delhi-based firm, directors*. The Hindu: thehindu.com/news/national/child-pornography-cbi-books-delhi-based-firm-directors/article31734988.ece
- Passoff, M. (2020, March 17). *Facebook At Center of Storm Over Child Sexual Exploitation Online*. proxypreview: <https://www.proxypreview.org/2020/contributor-articles-blog/2020/3/16/facebook-at-center-of-storm-over-child-sexual-exploitation-online>

- Peterson, B. (2013). A Legal Perspective of Child Sexual Abuse in the Caribbean, with a Focus on Trinidad and Tobago. In A. Jones, *Understanding Child Sexual Abuse* (pp. 51-75). London: Palgrave Macmillan.
- Pfefferkorn, R. (2020). Client Side Scanning and Winnie-The-Pooh Redux. Stanford Law School: <http://cyberlaw.stanford.edu/blog/2020/05/client-side-scanning-and-winnie-pooh-redux-plus-some-thoughts-zoom>
- Polofsky, J. (2012, January 20). *U.S. accuses Megaupload for copyright infringement*. Reuters: <https://www.reuters.com/article/us-usa-crime-piracy/u-s-accuses-megaupload-of-copyright-infringement-idUSTRE80I24220120119>
- Reuters. (2019, July 12). *Chile removes statute of limitations on child sex abuse amid Church crisis but new law not retroactive*. The Japan Times: <https://www.japantimes.co.jp/news/2019/07/12/world/crime-legal-world/chile-removes-statute-limitations-child-sex-abuse-amid-church-crisis-new-law-not-retroactive/>
- Ripeanu, M., Lamnitchi, A., & Foster, I. (2002). Mapping the Gnutella Network. *IEEE Internet Computing*, 50-57.
- Roberts, A. P. (n.d.). *The Dangers of Peer-to-Peer Sharing: How Innocent Users Can Be Arrested for Illegal Child Pornography*. Roberts Law Group, PLLC: <https://www.robertslawteam.com/Criminal-Defense-Overview/Articles/The-Dangers-of-Peer-to-Peer-Sharing-How-Innocent-Users-Can-Be-Arrested-for-Illegal-Child-Pornography.shtml>
- Rokundo, S. (2016). Intolerable Acts: An Analysis of the Law Relating to Online Child Pornography in Uganda. *Pretoria Student Law Review*, 124-142.
- Salian, D., & Khatun, S. (2020). Legal Frame Work on Child Pornography: A Perspective. In B. Shetty, P. Shetty, & A. Shetty, *Digital Forensic Science* (pp. 1-12). Intechopen.
- Sawyers, P. (2018, September 03). *Google releases AI powered Content Safety API to identify more Child Abuse Images*. Venture Beat: <https://venturebeat.com/2018/09/03/google-releases-ai-powered-content-safety-api-to-identify-more-child-abuse-images/>
- Schulman, R., & Bankston, K. (2017, July 31). *Deciphering the European Encryption Debate: France*. New America: <https://www.newamerica.org/oti/blog/deciphering-european-encryption-debate-france/>
- Senseney, H. (1998). Interpreting the Communications Assistance for Law Enforcement Act of 1994: The Justice Department Versus the Telecommunications Industry & (and) Privacy Rights Advocates. *Hastings Communications and Entertainment Law Journal*, 665-698.

- Sharma, N. (2020, January 24). *The PinkCity Post*. Man arrested for sharing child pornography in WhatsApp group: <https://www.pinkcitypost.com/man-arrested-for-sharing-child-pornography-in-whatsapp-group/>
- Singh, N. (2019, November 15). *CBI sets up online Child Sexual Abuse and Exploitation (OCSAE) Prevention/Investigation unit*. DD News: <http://ddnews.gov.in/national/cbi-sets-online-child-sexual-abuse-and-exploitation-ocsa-prevention-investigation-unit>
- Slatz, A., & Cheong, I. M. (2020, February 03). *EXCLUSIVE: Pedophiles are using Twitter to share child porn*. The Post Millennial: <https://thepostmillennial.com/exclusive-pedophiles-are-using-twitter-to-share-child-porn>
- Soares, E. (2008, July 02). *Brazil: Child Pornography to Be Criminalised*. Library of Congress: <https://www.loc.gov/law/foreign-news/article/brazil-child-pornography-to-be-criminalized/>
- Sothesian, D. (2013). *Dotcom's Mega Mess: New Zealand's Role in a foreign Search Warrant Request (Thesis)*. Wellington: Faculty of Law, University of Wellington.
- Thaver, M. (2020, January 28). *US alert for India: 25,000 child porn cases uploaded in five months*. The Indian Express: <https://indianexpress.com/article/india/child-pornography-india-ncmec-us-report-6238603/>
- thorn.org. (2014, April 30). *Redefining "Child Pornography"*. Thorn: <https://www.thorn.org/blog/redefining-child-pornography/>
- thorn.org. (n.d.). *Child Pornography and Abuse Statistics*. Thorn: <https://www.thorn.org/child-pornography-and-abuse-statistics/>
- U.S. Department of Justice. (2016, April). *The National Strategy for Child Exploitation Prevention and Interdiction: A Report to Congress*. U.S. Department of Justice: <https://www.justice.gov/psc/file/842411/download>
- Umeda, S. (2016, May). *Government Access to Encrypted Communications: Japan*. Library of Congress: <https://www.loc.gov/law/help/encrypted-communications/japan.php>
- UNICEF. (2015). *Guidelines for Industry on Child Online Protection*. UNICEF: https://www.unicef.org/csr/files/COP_Guidelines_English.pdf
- UNICEF & GSMA. (2016). *Notice and Takedown*. https://www.unicef.org/csr/files/Notice_and_Takedown_English.pdf
- University of Waikato. (2019, December 12). *Government's power to order decryption must respect privacy*. Scoop Politics: <https://www.scoop.co.nz/stories/PO1912/S00166/governments-power-to-order-decryption-must-respect-privacy.htm>

- US Department of Labor. (2013). *Honduras*. Ref World: <https://www.refworld.org/pdfid/5448a6170.pdf>
- Veerappan, D. (2020, May 21). *Man arrested for sharing child pornographic material through ..* The Times of India: <https://timesofindia.indiatimes.com/city/chennai/man-arrested-for-sharing-child-pornographic-material-through-whatsapp/articleshow/75865879.cms>
- Walshe, P. (2016, May). *Notice and Takedown: Company policies and practices to remove online child sexual abuse material*. UNICEF: https://www.unicef.org/csr/files/Notice_and_Takedown_English.pdf
- WePROTECT Global Alliance. (2018). *Global Threat Assessment 2018: Working together to end the sexual exploitation of children online*, 2.
- WeProtect Global Alliance. (2020). *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse*. <https://www.gov.uk/government/publications/voluntary-principles-to-counter-online-child-sexual-exploitation-and-abuse>
- Xinhua. (2019, October 26). *China Focus: China adopts law on cryptography*. Xinhuanet: http://www.xinhuanet.com/english/2019-10/26/c_138505655.htm
- Zhang, L. (2007). *China: Children's Rights*. Law Library of Congress.
- Zhou, Z. (2016, January 23). *China's Comprehensive Counter-Terrorism Law*. The Diplomat: <https://thediplomat.com/2016/01/chinas-comprehensive-counter-terrorism-law/>



CyberPeace
— Foundation —

www.cyberpeace.org