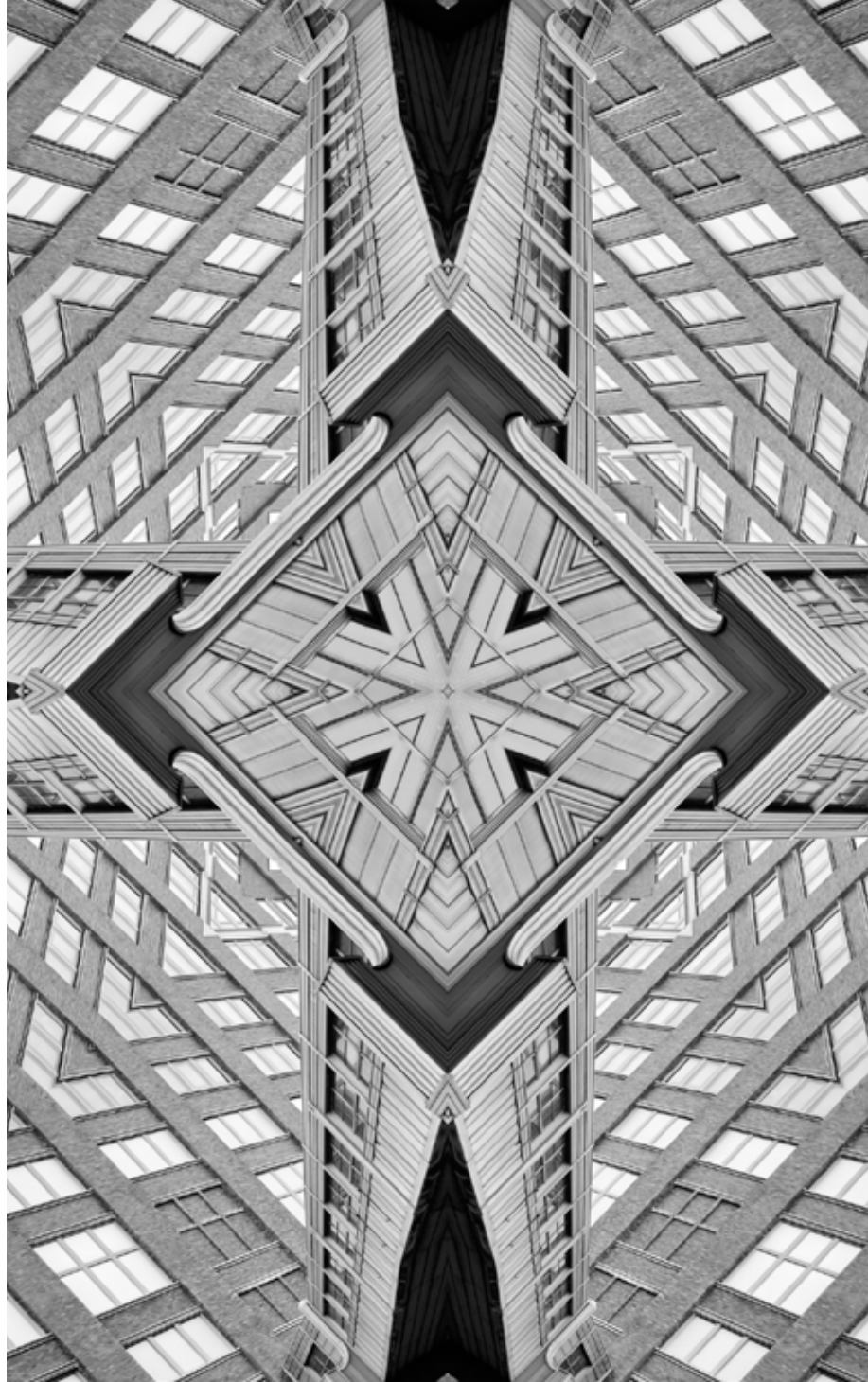


Issue

Brief

ISSUE NO. 557
JUNE 2022



Promoting Child Safety Online in the Time of COVID-19: The Indian and Australian Responses

Anirban Sarma

Abstract

Since the outbreak of the COVID-19 pandemic in early 2020, there has been a surge in cases of online child sexual abuse and exploitation (OCSAE) in many parts of the world. This brief discusses the cases of India and Australia. It examines their efforts to combat the increased incidence of OCSAE resulting from greater use of the internet as movement was restricted in response to the pandemic. The brief focuses on India and Australia as both have demonstrated a commitment to promoting child rights and safety and rank high in the 2020 Child Online Safety Index. They are also collaborating on a range of technology and cyber-cooperation initiatives. The brief assesses the implementation and potential effectiveness of key laws, mechanisms, strategies and programmes deployed in the two countries beginning in February 2020, and proposes areas of collaboration.

In recent years, there has been a steady growth in Internet use by children and youth in many parts of the world. In 2017, 50 percent of the global population and around 67 percent of 15- to 24-year-olds used the Internet. As of 2019, it was estimated that one of every three children under 18 years was an Internet user, and one in every three Internet users was a child under 18 years of age.¹ Since early 2020, even more children have begun to spend time on the Internet—for learning, socialisation, and entertainment—as a result of the widespread lockdowns and school closures that were implemented by governments to attempt to contain the COVID-19 outbreak.² As UNICEF has observed, the increase in children’s screen time poses severe risks to their online safety, and heightens the potential exposure to harmful behaviour and content.³

Globally, cases of online sexual abuse and exploitation of children have risen since the pandemic began.⁴ In India, for instance, cybercrimes against children in 2020 rose by more than 400 percent over the previous year. Nearly 90 percent of these crimes were related to the publication or transmission of content depicting children in sexually explicit acts.⁵ The shift to online schooling, the use of educational apps, and the increased use of social media have been found to pose threats to the online safety of children in India.^{6,7}

These trends are not unique to India. In the European Union (EU), the Europol reported a “steep increase” in online “grooming” activities^a and a “considerable increase” in the sharing of child sexual abuse materials (CSAM) in 2020-21.⁸ In the United States (US), OCSAE cases more than doubled in the first half of 2020, compared to the first half of 2019.⁹ The UK-based watchdog, Internet Watch Foundation, has observed that 2021 was the worst year on record for child sexual abuse online.¹⁰ Australia too, saw a 90-percent increase in online illegal content between 2019 and 2020, the bulk of it consisting of CSAM.¹¹

a Online grooming refers to the process of befriending a child online and building their trust with the intention of exploiting or harming them. The harm caused by grooming could take the form of sexual abuse, both in person or online, or exploitation to obtain sexually explicit images or videos of the child.

Globally, peer-to-peer and darknet networks are the main channels for accessing and distributing CSAM non-commercially. To a minor extent, certain forms of commercial exploitation, such as the livestreaming of abuse, also contribute to the proliferation of CSAM.¹²

UNICEF has identified six distinct, but sometimes overlapping, types of online risks for children: cyberbullying, online sexual abuse, online sexual exploitation, cyber extremism or radicalisation, online commercial fraud, and habit formation and online enticement to illegal behaviours.¹³

This brief focuses on an amalgam of the second and third categories, referred to collectively as online child sexual abuse and exploitation, or OCSAE. OCSAE could include a range of activities: producing, distributing and viewing materials (such as photographs or videos) related to the abuse of children; luring children into sexual chats or generating explicit content; grooming and enticing children through sustained communication to meet the abuser in the real world; exhibitionism by the abuser designed to shock or harass a child; and introducing or permitting a child to engage in prostitution or sexual trafficking over the Internet.¹⁴

This brief examines the efforts undertaken in India and Australia to combat the wave of OCSAE amidst the COVID-19 pandemic. It assesses the implementation of key laws, mechanisms and programmes that have sought to address OCSAE in the two countries since February 2020,^b and explores the potential effectiveness of new legislation or strategies introduced thereafter. It also identifies gaps, recommends possible corrective measures, and proposes areas in which India and Australia could cooperate to strengthen child safety online.

^b Although India and Australia detected their first cases of COVID-19 in late January 2020, it was only in February that the outbreak was formally recognised by both countries as a health emergency at scale, after which response actions were initiated. This is why this brief uses February 2020 as the starting point for its analysis.

Focus on India and Australia

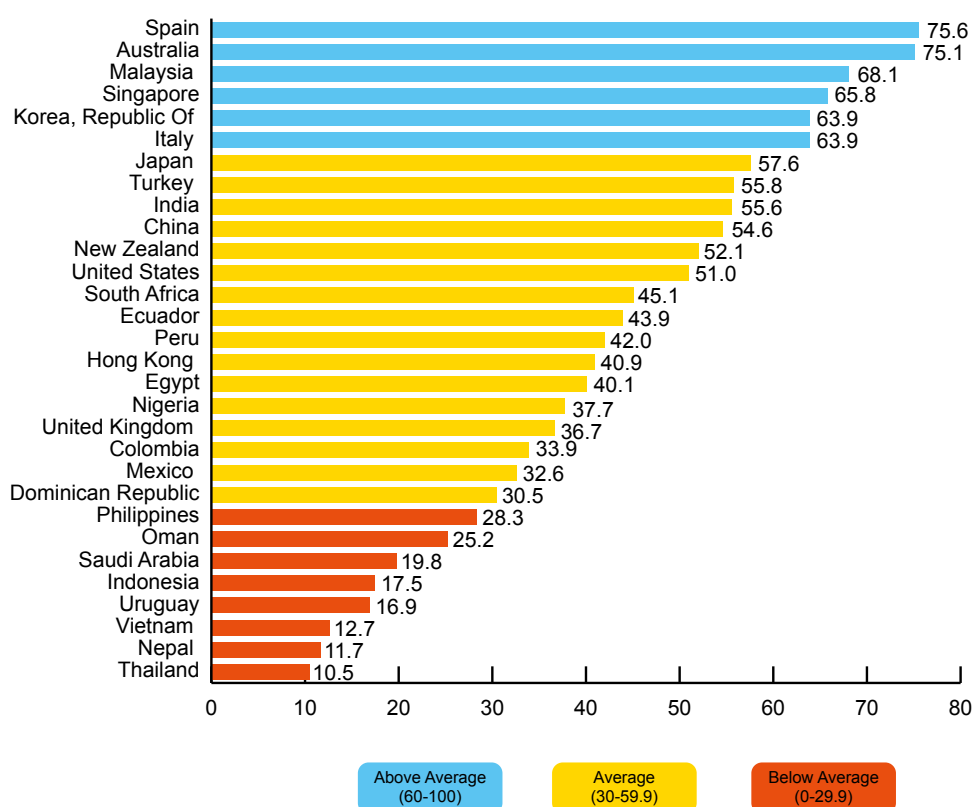
The choice of India and Australia as subjects of analysis for this study has been guided by three related factors.

International commitment to child rights: Both countries were early ratifiers of the UN Convention on the Rights of the Child (CRC), which came into effect in September 1990 and is the only binding international legal instrument that seeks to protect children's rights in their entirety.¹⁵ India and Australia have also acceded to the second Optional Protocol to the CRC on the Sale of Children, Child Prostitution and Pornography (effective since 2002),¹⁶ which further signals their commitment to promote children's rights and safety.^c

Child online safety status: The 2020 Child Online Safety Index (COSI), a survey of 30 countries conducted during the first year of the pandemic, ranked both Australia and India among the top 10 countries with the "best online safety for children".¹⁷ While Australia ranked second on this parameter, India ranked ninth (see Figure 1). With respect to the "extent of cyber-risks" faced by children, however, India ranked second while Australia ranked eleventh, indicating that the former experiences a higher volume of risks but the latter appears to deal with them more effectively.

^c It has since been affirmed that the CRC's provisions – such as Article 19, which outlines "forms of exploitation, including sexual abuse" – also apply to ICT-enabled or online forms of violence. The second Optional Protocol further strengthens the CRC's provisions vis-à-vis both online and offline offences against children.

**Figure 1:
2020 Child Online Safety Index: Which countries have the best online safety for children?**



Source: DQ Institute, <https://www.dqinstitute.org/wp-content/uploads/2020/02/2020COSIReport.pdf>

The gap between the two countries widens considerably if their *overall* cyber-safety is considered (including the online safety of adults and the cybersecurity of businesses, governments, and infrastructure). For instance, the SEON Global Cyber-Safety Index 2020, which analyses data from a range of national and global cybersecurity indices and indicators, ranked Australia eighth and India 61st.¹⁸ Seen in conjunction with the COSI, this indicates that India has been able

Focus on India and Australia

to address cybercrimes against children more effectively than other such crimes in general, while Australia has more robust systems to address cybercrimes across categories.

Growing bilateral cyber and technology cooperation: In recent years, India and Australia have cooperated more closely on cyber and technology issues. This is demonstrated by the Australia–India Cyber and Critical Technology Partnership, other ongoing initiatives such as the two countries’ annual Cyber Policy Dialogue, and new working groups on cybersecurity cooperation and information and communication technologies (ICTs).¹⁹ Given their commitment to promoting child safety online, it would be possible for both countries to work together to build a safer and more secure cyberspace for children.

India has historically given less attention to online child safety than Australia in its bilateral or multilateral engagements. While India has had an agreement with the American National Centre for Missing and Exploited Children since 2019 to receive reports about in-country instances of OCSAE, its other international engagements have generally sought to strengthen cybersecurity, and not online child safety, in particular.^{20,21} By comparison, in 2021 alone, Australia entered into online child safety-related bilateral agreements with South Korea and Fiji, and it continues to be an active governmental member of the WeProtect Global Alliance to prevent OCSAE.²²

“Both India and Australia were early ratifiers of the UN Convention on the Rights of the Child (CRC), which came into effect in September 1990.”

India has developed a progressive legal framework for protecting children online. While certain acts and legal provisions, especially those enacted after 2000, often explicitly draw attention to crimes against children that involve the use of ICTs, others that describe offences against children in more generic terms are now understood to apply to virtual spaces as well.

The most frequently cited and applied laws for protecting children against OCSAE in India are the Protection of Children against Sexual Offences (POCSO) Act, 2012,^d and the Information Technology (Amendment) Act, 2008. The latter significantly broadened the scope of the Information Technology Act, 2000, by identifying online offences to which children are most vulnerable. Further, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, calls on social media intermediaries to identify CSAM on their platforms, flag such content, and communicate to users trying to access the content that it has been identified as inappropriate. Additionally, relevant sections of the Indian Penal Code (1860) and the Immoral Traffic Prevention Act (1956) are drawn upon to report certain instances of OCSAE, such as the sale and circulation of obscene materials; the sexual harassment, defamation and criminal intimidation of children; and online extortion and child trafficking.²³

India has responded to the rise in OCSAE during the pandemic in four principal ways: upscaling its promotion of existing mechanisms for reporting online crimes against children; implementing a crackdown on the transmission and hosting of CSAM online, particularly on social media platforms; sensitising schools; and promoting capacity development for law enforcement agencies and other stakeholders within the OCSAE prevention ecosystem, as well as the technological capacity for addressing threats to children.

d The POCSO Act was amended in 2019 to expand the definition of “child pornography” to include “digital or computer-generated” CSAM, and to empower the central government to frame rules for how pornographic material in any form could be deleted, destroyed, or reported to the appropriate authority.

Promoting existing mechanisms for reporting OCSAE

Both of India's principal mechanisms for self-reporting OCSAE have been in operation even before COVID-19. In 2017, the National Commission for Protection of Child Rights (NCPCR) set up the POCSO e-Box, an online complaint management system that allows victims or their representatives to report cases of OCSAE. In 2019, the government launched the National Cybercrime Reporting Portal for the public to report instances of cybercrime, with a special focus on those committed against women and children. As police and public order are state subjects,^e once reported, records of these crimes are shared with state-level law enforcement agencies (LEAs) for action.

Faced with a sharp rise in OCSAE since early 2020, the NCPCR and the National Commission on Women have both revitalised efforts to advocate for the public use of these reporting platforms and to raise awareness about how the POCSO and IT Acts could address OCSAE. In this regard, programmes for outreach, stakeholder engagement, and consultation have been systematically rolled out since the pandemic began.²⁴ A key additional mechanism leveraged during this period involves the information-sharing agreement established in 2019 between the Indian National Crime Records Bureau (NCRB) and the American National Centre for Missing and Exploited Children (NCMEC). The NCRB has received regular 'tipline' reports^f about OCSAE from the NCMEC, which it has then shared with state-level LEAs through the National Cybercrime Reporting Portal, encouraging them to respond to these cases.²⁵

India's efforts to promote its OCSAE reporting mechanisms during the pandemic are laudable, but more needs to be done to raise public awareness about these measures. Inadequate knowledge about OCSAE and avenues for its redress has long been a challenge. This has translated to a low rate of self-reported crimes: the POCSO e-Box, for instance, received a mere 151 complaints in 2020-2021,²⁶ and only 1,102 cybercrimes against children have been reported on the National Cybercrime Reporting Portal in 2020.²⁷ In contrast, in 2020 the NCRB received 2,725,518 reports of OCSAE from the NCMEC.²⁸

e The State List is a list of 61 subjects in the Seventh Schedule to the Constitution of India. Only India's state governments have the exclusive power to legislate on matters relating to these subjects.

f The NCMEC's CyberTipline is a centralised reporting system for the online exploitation of children. It allows citizens and electronic service providers to report a wide range of actual and suspected instances of OCSAE, and related crimes against children. These reports could then be shared with national law enforcement agencies around the world in whose jurisdictions the offences may have occurred or originated.

Addressing spread of child sexual abuse materials on social media

In February 2020, a parliamentary committee submitted a report to the Rajya Sabha (upper house of parliament) on the issue of pornography and CSAM on social media, and its effects on children.²⁹ Among other recommendations, it called for social media intermediaries to report CSAM to Indian law enforcement agencies; for intermediaries and Internet Service Providers (ISPs) to identify and proactively take down CSAM; and permitting the breaking of end-to-end encryption to trace distributors of child pornography. In a similar spirit, a 2021 NCPCR study noted that stricter oversight and rule enforcement was needed for social media platforms as they could carry content that represented the online abuse of children.³⁰

These perspectives, and a long-running debate about the feasibility of weakening encryption for specific law enforcement purposes, have culminated in a controversial new legislation, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The new IT Rules stipulate that social media intermediaries must prohibit users of their platform from publishing or transmitting material that is “obscene, pornographic, paedophilic [...] or harmful to child[ren]”. Section 4(4) of the Rules enjoins upon intermediaries to use tech-based measures including automation tools to identify and flag CSAM, and curb user access to such content. More contentiously, intermediaries that primarily provide messaging services are now expected to help trace the originator of the information when there is a judicial order related to the “prevention, detection, investigation, prosecution or punishment” of offences involving CSAM or sexually explicit material.³¹

The IT Rules are problematic on several grounds. If social media platforms are to enable the traceability of content, they will have to break the end-to-end encryption used by many platforms. This will seriously compromise the security of all online communications on the platforms. While certain technical methods such as ‘hashing’^g or attaching originator information to messages have been proposed, these are by no means foolproof and will adversely affect communication privacy, and pose other practical limitations for platforms.

^g Hashing is an operation that converts a piece of information into a unique string of characters. While recovering the original text from its hash is not possible, when confronted with a legal order an online service provider (OSP) could compare a hash to all the other hashes in its database, enabling the identification of the relative and absolute originators of a message. This is detrimental to the security of communications as storing hashes of private and confidential messages could expose them to scrutiny by OSPs or by malicious actors capable of breaching the OSP’s systems.

There is now a broad consensus that, technically, it is not possible to weaken encryption for specific purposes while maintaining the previously high levels of security for other general purposes.³² Importantly, the IT Act as a whole does not empower the government to mandate technical changes to platforms, and therefore the very legality of the subsidiary IT Rules is questionable.³³ Finally, the Rules do not propose any clear mechanism for enforcing the traceability obligation. Thus, while in spirit the IT Rules seek to address OCSAE, it is difficult to see how they might be satisfactorily implemented without resolving these issues.

Sensitising schools

The Indian government's efforts to sensitise schools about online threats to children, including OCSAE, has formed a vital plank of its pandemic response, particularly in light of the transition to online classes after the nationwide closure of education institutions on 24 March 2020.³⁴ The NCPCR has been quick to develop and widely circulate a manual for safety in schools that now includes a compilation of all existing guidelines, laws and reporting mechanisms related to children's cyber safety, and provides a detailed blueprint for schools to frame cyber safety rules.³⁵ The Ministry of Education has undertaken similar initiatives on a national scale, releasing its *Guidelines for School Safety and Security* in 2021; and nodal bodies such as the Central Board for Secondary Education and National Council for Educational Research and Training, have released student-friendly handbooks on online child safety issues, and helped train teachers on cybersafety.³⁶

The aim of these initiatives is twofold—to place the onus on schools to orient administrators, teachers and IT personnel about the importance of cyber safety for children; and to educate children directly about measures for staying safe online. There is, however, a need to go further. State governments must ensure that these or similar tools are adopted across schools and boards at the state level. The creation of state cybersafety monitoring mechanisms for schools will lead to greater school-level implementation of such cyber guidelines.

Developing human and technical capacity

The training and sensitisation of LEA personnel, prosecutors and judicial officers under the Cyber Crime Prevention against Women and Children scheme operated by the Ministry of Home Affairs has continued apace during the pandemic. The aim is to improve the investigation and prosecution of online crimes against children. These ongoing efforts to strengthen human capacity are complemented by technology-based initiatives, particularly those undertaken by Big Tech firms to tackle OCSAE and other cybercrimes against children since the pandemic began. In India, for instance, both Google³⁷ and Facebook³⁸ have introduced product and policy changes, undertaken technical measures to remove CSAM from their platforms, and launched programmes to raise children's awareness about online safety.

“India has responded to the rise in online child sexual abuse during the pandemic by upscaling the promotion of its mechanisms for reporting.”

The Australian Response

According to a 2021 survey, two out of three people in Australia reported experiencing online sexual harm before turning 18, a rate higher than most other regions in the world.³⁹ The rise of OCSAE has partly been attributed to the pandemic, with experts remarking on the “perfect storm of conditions with more young people online than ever before and more apps and platforms available”.⁴⁰ Indeed, Australia witnessed a sharp spike in app downloads across all categories between the first and second quarters of 2020 – a phenomenon attributed to the Covid-19 outbreak. Mobile gaming apps in particular have consistently seen the highest number of downloads between the first quarter of 2020 and the second quarter of 2021, and they reached a peak of 213 million downloads in the second quarter of 2020, right after the pandemic began.⁴¹

Like India, Australia has a stringent legal framework at the federal and state levels to protect children online. Australia’s Enhancing Online Safety for Children Act (2015) has been the primary national legal instrument for countering a range of online harms for children. Divisions 273 and 274 of Australia’s Criminal Code criminalise the production and distribution of CSAM, and the country has also introduced legal measures to deal with online child grooming. Moreover, at the state and territory level, laws such as the Children and Young People Act (2008), Crimes (Child Sex Offenders) Act (2005), Care and Protection of Children Act (2007) and Child Protection Act (1999) all address offences that are now interpreted as being applicable to cyberspace.⁴²

Australia has responded to the surge in OCSAE since the outbreak of the pandemic in three ways. First, it has enacted a comprehensive new law, the Online Safety Act, 2021, that greatly strengthens existing measures for promoting online safety. Second, it has begun to implement a comprehensive National Strategy to Prevent and Respond to Child Sexual Abuse (2021-30) that involves a wide spectrum of stakeholders. Third, it is engaging with school systems, sensitising students, parents and educators about OCSAE and other online risks, and continuing to train law enforcement officers to address these risks.

The Australian Response

Enabling safer digital environments through the Online Safety Act

The aim of the Enhancing Online Safety for Children Act (2015) was to identify and remove online child cyberbullying material, and enforce measures to make social media a safer space for children. Australia's new Online Safety Act (2021) builds on these principles, extends them by including all citizens under its ambit, and, crucially, demands a high level of private sector compliance and cooperation to ensure online safety. Additionally, it gives the Australian eSafety Commissioner (or eSafety) new powers to require ISPs to block access to CSAM, and to regulate illegal and restricted content irrespective of where it is hosted.

The new Act makes online service providers (OSPs) more accountable for the safety of their users. It lays down a set of 'basic online safety expectations' (BOSE) to ensure user safety and compel service providers to be more proactive in tackling online harms such as OCSAE. Service providers are now required to prevent access to CSAM, and create easily comprehensible mechanisms for users to lodge complaints about unacceptable content. The Act also mandates the online industry to develop appropriate codes to detect and remove illegal content such as CSAM, failing which, eSafety could impose industry-wide standards to compel them to do so.⁴³ With eSafety asserting that it will prioritise the investigation of complaints about the most harmful material such as CSAM, OSPs with Australian end-users are likely to find themselves under pressure to revise their safety procedures and align them with the requirements of the BOSE, and the Act in general.

Broadly, even prior to the pandemic, Australian efforts to promote child safety online have sought to place a stronger onus on tech firms to act transparently and responsibly;⁴⁴ the Online Safety Act is consistent with that approach. The Act has largely been well-received within the country, and is being positioned as a mechanism that "places Australia at the international forefront in the fight against online abuse and harm."⁴⁵

Launching a National Strategy and Online Safety Youth Advisory Council

Parallel to the institution of the Online Safety Act, the Australian state and territory governments co-developed a pioneering National Strategy to Prevent and Respond to Child Sexual Abuse. The strategy is being envisaged as a holistic “nationally coordinated strategic framework” to address child sexual abuse.⁴⁶ With online child safety as a pillar, the strategy, in which the government is expected to invest over AUD 307 million (approx. USD 215 million), will be systematically implemented across Australia through an action plan that will run from 2021 to 2024 in the first instance.⁴⁷ Importantly, nearly one-fifth of the total outlay will be allocated for initiatives to be implemented directly by the Australian Federal Police to combat OCSAE by boosting its human and technological capacities.⁴⁸ As the potential generator of a second layer of preventive action beyond the Online Safety Act, the strategy is expected to play a key part in curbing OCSAE in Australia over the coming decade.

Additionally, in a bid to include children as equal partners in the fight against OCSAE, the Australian government is in the process of instituting an Online Safety Youth Advisory Council. It will consist of some 20 Australians 13 to 24 years of age, and will formally provide feedback to the government about online safety issues and measures to counter cyber-harms.⁴⁹ This feedback and consultation mechanism is an important adjunct to the national strategy, and will integrate at-risk stakeholders into the national decision-making process.

Sensitising stakeholders and building capacity

During the pandemic, Australia also continued existing efforts to sensitise stakeholders and build their capacity to combat OCSAE.

Much like the interventions of apex educational bodies in India, eSafety has consistently engaged with Australian school systems to promote a variety of information resources that target students, educators and parents. Its ‘School Community Engagement Plan’ has been in operation since February 2020, and the plan has successfully utilised the ‘eSafety Toolkit for Schools’ to raise public

The Australian Response

awareness about online risks including OCSAE, and mechanisms for reporting online crimes against children.⁵⁰ Besides, a second front for sensitisation has been provided by the Australian Federal Police, whose ThinkUKnow programme provides resources for parents and carers to help prevent OCSAE.⁵¹

Finally, the capacity development of law enforcement agencies has continued to be an important area of intervention. A 2021 survey of Australian police officers showed that they perceive “child abuse material and the sexual solicitation of children” as one of the most serious types of criminal offence (out of a list of 27), second only to “physical terrorist attacks”.⁵²

“Australia has responded to the surge in online child sexual abuse by, first, enacting a comprehensive Online Safety Act, 2021.”

Conclusion and Recommendations

India's and Australia's responses to OCSAE during the pandemic have several common strands. At the same time, they demonstrate fundamentally different strengths and points of focus. Overall, the Indian approach has been more activity-based, reactive, focused on emergency response and immediate goals, and inclined towards downstream stakeholder engagement. Australia's, meanwhile, has centred on the proactive enactment of new legislation and upstream policy engagement, designed to initiate immediate change and to work programmatically towards the implementation of long-term national strategies and plans. Both approaches have their merits, are complementary, and present opportunities for India and Australia to learn from each other and strengthen their OCSAE response systems.

The first two of the three recommendations are directed towards India, while the third proposes certain areas for bilateral cooperation between India and Australia.

Recommendation 1: Build awareness about OCSAE focusing on scale, visibility, and sustainability, and fast-track OCSAE cases.

Australian citizens appear to be more widely aware of their country's OCSAE reporting mechanisms and resources than their Indian counterparts. Awareness about Indian OCSAE prevention laws, resources and reporting processes remains limited despite the recent sensitisation drives conducted by local authorities.⁵³ Sensitisation efforts must therefore be strategic, visible, large-scale, and sustained, and should not be reduced to a response to a specific crisis like the pandemic. A phased 360-degree national awareness campaign supported by the traditional mass media could be a decisive first step. Concomitantly, mainstreaming modules on OCSAE and cyber hygiene into school computer science and sex education curricula—while ensuring that knowledge products and sensitisation materials are made available in multiple Indian languages—will go a long way towards educating students about online risks. Finally, given the large backlog of cases involving crimes against children,⁵⁴ every effort should be made to address registered OCSAE-related cases on a priority basis, and fast-track processes to prosecute the perpetrators of these crimes.

Conclusion and Recommendations

Recommendation 2: Ensure private sector cooperation and compliance for removing CSAM.

The fight against OCSAE cannot be won without the increased accountability, responsibility, and cooperation of ISPs and OSPs. India's IT Rules require greater clarity and a more sensitive appraisal of possible security and privacy implications before they can realistically be implemented by the social media intermediaries for whom they are intended. The draft amendments to the IT Rules⁵⁵—proposed on 6 June 2022 and currently open for public comment—suggest that online intermediaries, including social media intermediaries must inform their users of their rules, regulations, and privacy policy, and shall “cause the user of [their] computer resource not to host, display, upload, modify, publish, transmit, store, update or share” any content that qualifies as CSAM or is “harmful to child[ren]”. This is a positive step. Unfortunately, the tendentious clauses about traceability and decryption remain unchanged.


India has had little success persuading ISPs to cooperate with efforts to prevent access to CSAM.⁵⁶ In this regard, India could closely study Australia's Online Safety Act with its tough measures for enforcing compliance from among tech firms. In the first instance, India could design an ethical framework or set of codes for countering OCSAE in collaboration with the private sector. If compliance continues to be a challenge, it could consider enshrining in law both the right and well-defined mechanisms to remove CSAM and other harmful content from online platforms.

Recommendation 3: Put online child safety squarely on the agenda of India-Australia cyber-cooperation.

The ongoing cyber-initiatives between India and Australia provide a ready context for online child safety to be put on the agenda. The capacity development of LEAs and cyber officials to address OCSAE is an urgent common priority for both countries. A key area for capacity building ought to be the mapping of how CSAM offenders operate, and to distinguish between the distribution of CSAM on the clear web and the dark web. The use of analytical tools such as crime scripts could help better understand, detect, investigate, and prevent the

Conclusion and Recommendations

circulation of CSAM, and identify intervention points at which OCSAE could be disrupted.⁵⁷ In this regard, joint cyber drills, trainings, and the exchange of best practices could be carried out under the auspices of the Indian Cybercrime Coordination Centre, established in January 2020 and the new Australian Federal Police-led centre to combat cybercrime.

Finally, at the level of policy engagement, collaborative approaches for strengthening child safety online ought to become a standing thematic area under the annual India-Australia Cyber Policy Dialogue. The development of cyber norms and principles to address crimes against children could benefit not only India and Australia but the broader Indo-Pacific region. 

Anirban Sarma is Senior Fellow at ORF's Centre for New Economic Diplomacy (CNED).

- 1 UNICEF, *Growing up in a Connected World*, 2019, <https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf>
- 2 UNICEF, “Children at increased risk of harm online during global Covid-19 pandemic”, April 14, 2020, <https://www.unicef.org/press-releases/children-increased-risk-harm-online-during-global-covid-19-pandemic>
- 3 UNICEF, *Covid-19 and Its Implications for Protecting Children Online*, 2020, pp.1–2, <https://www.unicef.org/media/67396/file/COVID-19%20and%20Its%20Implications%20for%20Protecting%20Children%20Online.pdf>
- 4 WeProtect Global Alliance, *Global Threat Assessment 2021: Working Together to End the Sexual Abuse of Children Online*, 2021, <https://www.weprotect.org/global-threat-assessment-21/#report>
- 5 “Cyber crimes against children in 2020 rose over 400% from 2019: NCRB report”, *Hindustan Times*, November 14, 2021, <https://www.hindustantimes.com/india-news/cyber-crimes-against-children-in-2020-rose-over-400-from-2019-ncrb-report-101636876552282.html>
- 6 R Sujatha, “Safety concerns abound as online classes for children become a reality”, *The Hindu*, June 19, 2020, <https://www.thehindu.com/news/national/tamil-nadu/safety-concerns-abound-as-online-classes-for-children-become-a-reality/article31871840.ece>
- 7 Aashish Aryan, “Educational apps indulged in practices that put children’s privacy at risk: Report”, *The Economic Times*, May 30, 2022, <https://economictimes.indiatimes.com/tech/technology/educational-apps-indulged-in-practices-that-put-childrens-privacy-at-risk-report/articleshow/91893218.cms?from=mdr>
- 8 Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2021*, https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf
- 9 Dustin Racioppi, “‘People don’t want to talk about it’, but reports of kids being exploited online have spiked during coronavirus pandemic”, *USA Today*, October 26, 2020, <https://www.usatoday.com/story/news/nation/2020/10/22/coronavirus-child-abuse-nj-online-child-exploitation-reports-increase/6004205002/>
- 10 Ian Smith, “Covid lockdowns saw a record rise in online child sexual abuse reports, says watchdog”, *EuroNews*, January 14, 2022, <https://www.euronews.com/next/2022/01/14/covid-lockdowns-saw-a-record-rise-in-online-child-sexual-abuse-reports-says-watchdog>
- 11 Helena Burke, “Covid-19 lockdowns cause disturbing spike in online child exploitation activity in Australia”, *News.com Australia*, December 9, 2021, <https://www.news.com.au/national/crime/covid19-lockdowns-cause-disturbing-spike-in-online-child-exploitation-activity-in-australia/news-story/a8a2e904ae7f4704bc4484e81d470890>

- 12 Europol, “Child Sexual Exploitation”, <https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/child-sexual-exploitation>
- 13 UNICEF, *Child Online Protection in India*, 2016, https://www.icmec.org/wp-content/uploads/2016/09/UNICEF-Child-Protection-Online-India-pub_doc115-1.pdf
- 14 K Sanjay Kumar, *Is Your Child Safe?* (Kozhikode: The Book People, 2017), pp.46–58
- 15 UNOHCHR, *Convention on the Rights of the Child*, <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>
- 16 UNICEF, *Child Safety Online: Global Challenges and Strategies – Technical Report*, 2012, pp.53–54, https://www.unicef-irc.org/publications/pdf/ict_techreport3_eng.pdf
- 17 DQ Institute, *2020 Child Online Safety Index*, 2020, <https://www.dqinstitute.org/wp-content/uploads/2020/02/2020COSIReport.pdf>
- 18 Gergo Varga, “Global cybercrime report: Which countries are most at risk?”, SEON, 2020, <https://seon.io/resources/global-cybercrime-report/>
- 19 Brijesh Singh, “Common values, shared threats in India–Australia cyber security ties”, *The Indian Express*, April 27, 2022, <https://indianexpress.com/article/opinion/columns/common-values-shared-threats-in-india-australia-cyber-security-ties-7888890/>
- 20 Jaya Menon, “Why India lags in tackling online child sex abuse”, *The Times of India*, February 7, 2020, <https://timesofindia.indiatimes.com/city/chennai/why-india-lags-in-tackling-online-child-sex-abuse/articleshow/73993417.cms>
- 21 Leilah Elmokedam and Saumyaa Naidu, “Mapping of India’s cyber security-related bilateral agreements”, Centre for Internet and Society, December 29, 2016, <https://cis-india.org/internet-governance/blog/india-cyber-security-bilateral-agreements-map-dec-2016>
- 22 eSafety Commissioner, Australian Government, “International leadership and collaboration”, <https://www.esafety.gov.au/key-issues/tailored-advice/international#international-engagements>
- 23 NCPCR, FIRE and iProBono, *Child Victims of Cyber Crime: A Legal Toolkit*, 2017, <https://ncpcr.gov.in/showfile.php?lang=1&level=1&&sublinkid=1298&lid=1519>
- 24 Press Information Bureau, “Steps taken for the cyber safety of women and children”, July 22, 2021, <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1737762>
- 25 Press Information Bureau, “Measures to ensure safety and security of women and children on online platforms”, March 23, 2022, <https://pib.gov.in/PressReleasePage.aspx?PRID=1808686>
- 26 Press Information Bureau, “POCSO e-Box”, August 5, 2021, <https://pib.gov.in/PressReleasePage.aspx?PRID=1742816#:~:text=As%20per%20the%20information%20received,complaints%20have%20been%20addressed%20conclusively>

- 27 Press Information Bureau, “Measures to ensure safety and security of women and children on online platforms”
- 28 Paul Bischoff, “The rising tide of child abuse content on social media”, January 11, 2022, *Comparitech*, <https://www.comparitech.com/blog/vpn-privacy/child-abuse-online-statistics/>
- 29 Parliament of India, *Report of the Adhoc Committee of the Rajya Sabha to Study the Alarming Issue of Pornography on Social Media and Its Effect on Children and Society as a Whole*, February, 2020, https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/71/140/0_2020_2_16.pdf
- 30 NCPCR, *Effects (Physical, Behavioural and Psycho-Social) of Using Mobile Phones and Other Devices with Internet Accessibility by Children*, July 2021, <https://ncpcr.gov.in/showfile.php?lang=1&level=1&&sublinkid=2145&lid=2044>, p.20
- 31 Ministry of Electronics and IT, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules*, 2021, https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf
- 32 Anirudh Burman and Prateek Jha, *Understanding the Encryption Debate in India*, Carnegie India, 2021, <https://carnegieindia.org/2021/09/13/understanding-encryption-debate-in-india-pub-85261>
- 33 Torsha Sarkar et al, *On the Legality and Constitutionality of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code), Rules, 2021*, Centre for Internet and Society, <https://cis-india.org/internet-governance/legality-constitutionality-il-rules-digital-media-2021>
- 34 Jeffrey Kettleman and Kai Schultz, “Modi orders 3-week total lockdown for all 1.3 billion Indians”, *The New York Times*, March 24, 2020, <https://www.nytimes.com/2020/03/24/world/asia/india-coronavirus-lockdown.html>
- 35 Ambika Pandit, “NCPCR dos and don’ts for kids’ cyber safety”, *Times of India*, September 17, 2021, <https://timesofindia.indiatimes.com/india/ncpcr-dos-donts-for-kids-cyber-safety/articleshow/86186730.cms>
- 36 Ministry of Education, Government of India, *Compilation of Initiatives / Actions Taken to Mitigate the Effect of Covid-19 Pandemic on Education of School Children*, 2021, https://www.education.gov.in/sites/upload_files/mhrd/files/DOSEL_COMPILATION_ON_COVID_ACTIVITIES.pdf
- 37 “Google launches kids safety programme in India”, *The Economic Times*, August 25, 2021, <https://economictimes.indiatimes.com/tech/technology/google-introduces-global-kids-safety-programme-in-india/articleshow/85621829.cms>
- 38 “Unicef India, Facebook launch initiative to create safe online environment for children”, *The Hindu Business Line*, August 10, 2021, <https://www.thehindubusinessline.com/info-tech/unicef-india-facebook-launch-initiative-to-create-safe-online-environment-for-children/article35829055.ece>

- 39 WeProtect Global Alliance, *Global Threat Assessment 2021: Working Together to End the Sexual Abuse of Children Online*, 2021
- 40 Caitlin Fitzsimmons, “Australia among the worst for online sexual harm to children”, *The Sydney Morning Herald*, October 19, 2021, <https://www.smh.com.au/national/australia-among-the-worst-for-online-sexual-harm-to-children-20211018-p590xt.html>
- 41 “Number of mobile app downloads in Australia from 1st quarter 2020 to 2nd quarter 2021, by category’, *Statista*, <https://www.statista.com/statistics/1282725/australia-quarterly-app-downloads-by-category/>
- 42 “Australian child protection legislation”, CFA Resource Sheet, March 2018, <https://aifs.gov.au/cfca/publications/australian-child-protection-legislation>
- 43 Australian Government | eSafety Commissioner, “Learn about the Online Safety Act”, <https://www.esafety.gov.au/whats-on/online-safety-act#:~:text=>
- 44 Aditi Agrawal, “Don’t introduce end-to-end encryption’ UK, US and Australia ask Facebook in an open letter”, *MediaNama*, October 4, 2019, <https://www.medianama.com/2019/10/223-us-uk-australia-facebook-encryption/>
- 45 Ellen Ransley, “Online Safety Act to tackle cyber-bullying and child sex abuse”, *The West Australian*, January 23, 2022, <https://thewest.com.au/news/online-safety-act-to-tackle-cyber-bullying-and-child-sex-abuse-c-5413352>
- 46 Australian Government, National Office for Child Safety, “National Strategy to Prevent and Respond to Child Sexual Abuse”, <https://childsafety.pmc.gov.au/what-we-do/national-strategy-prevent-child-sexual-abuse>
- 47 *National Strategy to Prevent and Respond to Child Sexual Abuse 2021–2030*, <https://childsafety.pmc.gov.au/sites/default/files/2021-10/national-strategy-2021-30.pdf>
- 48 “Media Release – Prime Minister: National Strategy to Prevent and Respond to Child Sexual Abuse”, <https://www.pm.gov.au/media/national-strategy-prevent-and-respond-child-sexual-abuse>
- 49 Campbell Kwan, “Australia to establish youth advisory council for countering online child exploitation”, *ZDNet*, December 15, 2021, <https://www.zdnet.com/article/australia-to-establish-youth-advisory-council-for-countering-online-child-exploitation/>
- 50 eSafety, *School Community Engagement Plan*, February, 2020, https://www.esafety.gov.au/sites/default/files/2020-02/engage_1_-_school_community_engagement_plan.pdf
- 51 Australian Federal Police, “AFP urges parents and carers to prepare for digital milestones”, February 2, 2022, <https://www.afp.gov.au/news-media/media-releases/afp-urges-parents-and-carers-prepare-children-digital-milestones>

Endnotes

- 52 Cassandra Cross et al, *Responding to Cybercrime: Perceptions and Need of Australian Police and the General Community*, Australian Institute of Criminology, 2021, https://www.aic.gov.au/sites/default/files/2021-08/CRG_Responding%20to%20cybercrime_0.pdf
- 53 Sonal Kellogg, “POCSO Act: Only 13.7% TN children aware, Bihar has almost nil awareness”, *The News Minute*, September 15, 2020, <https://www.thenewsminute.com/article/pocso-act-only-137-tn-children-aware-bihar-has-almost-nil-awareness-133077>
- 54 “Over 2.26 lakh POCSO cases pending in fast-track courts, UP has 60,000”, *The Wire*, March 26, 2022
- 55 Ministry of Electronics and IT, *Proposed Draft Amendments to the IT Rules, 2021*, June 06, 2022, <https://www.meity.gov.in/writereaddata/files/Press%20Note%20dated%206%20June%2022%20and%20Proposed%20draft%20amendment%20to%20IT%20Rules%202021.pdf>
- 56 Alice Saju, “Online child sexual abuse: Industry players ignore government fiat on partnering IWF”, *The Hindu Business Line*, January 3, 2021, <https://www.thehindubusinessline.com/news/tata-communication-only-isp-to-have-partnered-with-iwf-to-prevent-child-sexual-abuse/article33479648.ece>
- 57 Beniot LeClerc et al, *Child Sexual Abuse Material on the Darknet: A Script Analysis of How Offenders Operate*, Australian Institute of Criminology, May 2021, https://www.aic.gov.au/sites/default/files/2021-05/ti627_csam_on_the_darknet.pdf



Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. Fax : +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org