IJM

International Justice Mission
Submission On:

Statutory Review of the Online Safety Act 2021

Table of Contents

Global Survivor Network - Comments on the Statutory Review of Australia's *Online Safety Act 2021*

To: Members of the Australian Parliament and Government leaders

We are the Global Survivor Network: an international group of survivors shaping and leading a movement to protect people from violence. As survivors of online sexual exploitation, we have come together so that through our example and collective voice, this painful and harmful abuse does not happen to more children. **We ask you to listen to our stories and our suggestions** as you work to strengthen Australia's *Online Safety Act*.

As survivors, **we are grateful** for Australia's leadership in regulating online safety and the ongoing work of the eSafety Commissioner in making digital platforms more accountable and transparent and supporting industry to develop safer online products. We appreciate your government's commitment to further improving online safety through the statutory review of the Online Safety Act. In undertaking this review, we ask that you consider seriously the experience and expertise of those who have first-hand knowledge of online harm. We have experienced the abuse and have been seeking justice for it. We want you to know how such acts affect us, not just physically but mentally and socially. It hurts our families and our communities. We thank you for listening to our voices and we hope you hear our suggestions.

We believe that it is very important to place responsibility for online safety and **hold accountable** online platforms like Meta, Skype, and others, who profit from their users. Digital service providers owe a **duty of care** to all children and adults who experience violence and abuse through the use of their platforms and services. We agree with the UN Committee on the Rights of the Child that **the rights of *every child* must be respected, protected and fulfilled in the digital environment, even where the children do not themselves access the internet.** Tech companies have the expertise to develop and deploy technology to ensure that their platforms and services are not used to cause harm. We know that they created these platforms for good, so they should find ways to prevent abuse from occurring on their platforms. We grieve for the children and adults who experience violence on their platforms.

We have experienced different forms of online sexual exploitation such as livestreamed sexual abuse and production of child sexual abuse materials in exchange for money received by facilitators from online paying customers. We experienced this abuse as children, and it continues to impact our lives. We ask the Australian Government to require that digital service providers make the **best interests of the child** a primary consideration in all actions that affect children and through every aspect of the design, development, management, implementation and use of digital platforms. This means requiring companies to prevent child sexual abuse material from ever entering these platforms, preventing victimisation from the very beginning. The best interests of the child should take priority over the commercial interests of technology companies.

We ask that digital platforms be required to have accurate systems that **detect when child sexual exploitation and abuse** content is shared using their platforms – especially because children, and not just adults, use and are impacted by their services. Tech companies should be able to detect and take action immediately and **block accounts** that use the platforms to abuse children. We also specifically ask that digital services be held accountable for **livestreaming child sexual abuse** – that such criminal activity be

proactively detected and disrupted on their platforms. If possible, applications that do not detect and stop the abuse should be shut down from public access.

> *"I am one of the survivors who is ready to talk about our experiences, I want to legislate the cessation of online sexual exploitation such as livestreams on Facebook or any app. I do not want women to experience more and even men get that kind of abuse because it's not a joke. I am asking for help so that I can process how to stop this abuse. Everyone needs protection. Every person performing this abuse must be stopped or monitored." – Diana*, 20-year-old survivor (13 years old at the time of abuse).*

Early detection by platforms helps to rescue the victims and to prevent them from further abuse. If digital platforms do not take immediate action, more young people will be abused, and the effects suffered by the victims will be worse.

A lot of young people have been abused and many of them have died by suicide because of their trauma. Survivors of online abuse often suffer severe trauma. It affects their mental, physical and emotional health, it affects their future, it also affects their family life. We don't want children to experience this – especially our future children. Its effects are grave and our recovery was not easy.

> "*Even after I was rescued, I had suicidal thoughts and most of my suicide attempts happened in the aftercare shelter I was brought to. My mind was unstable. Staff there said that I had the loudest laughter during activities. But I would bang my head against the bathroom walls when I am alone, bang my head against my room walls during a quiet midnight while everyone is fast asleep. I would cover my whole face with a thick pillow and try to suffocate myself while crying." Ruby, 16 years old when trafficked.*

Digital service providers should prioritise the protection of children and build their platforms and services **safe by design**. They should build in safety features so that platforms are unable to produce, capture, render or distribute child sexual abuse material.

We are grateful for the protections already in the *Online Safety Act* and that they will be further strengthened through this review. We also ask the Government to make sure that there is **strong enforcement** of those provisions. When companies fail to meet their obligation to prevent misuse of their platforms and to ensure protection from online harms, they should be required to pay for the consequences of their failure through **high penalties**.

We urge the Australian Government to include survivor consultation while drafting legislation as a critical component to informing policy decisions. As individuals with lived experience, we can provide real examples of how abuse and exploitation happen on these platforms, and what steps are necessary to take in order to make sure no children are ever exploited the way we were.

We are so glad that the Australian Government is reviewing the Online Safety Act to ensure that it is effective in protecting people from online harm and abuse. Australia's online safety laws have served as an inspiration for other countries to enact similar laws to protect children and other vulnerable people in the fight against online sexual exploitation. We urge you to prioritise child protection, further strengthen Australia's online regulation and require technology companies to meet their duty of care to prevent online harm.

Signed:

Malone* Survivor of OSEC, Philippines Survivor Network
Azalea* Survivor of OSEC, Philippines Survivor Network
Solenn* Survivor of OSEC, Philippines Survivor Network
Jaika*, Survivor of OSEC, Philippines Survivor Network
Nicole*, Survivor of OSEC, GSN Leadership Council
Ruby*, Survivor of OSEC, GSN Leadership Council
Godwin, Survivor: GSN Leadership Council
Betzi*, Survivor: GSN Leadership Council
Kumar, Survivor: GSN Leadership Council
Lillian, Survivor: GSN Leadership Council

**pseudonyms, to protect the identities of survivors of online sexual exploitation of children. Survivors from the PSN are joined by survivors from the GSN Leadership Council, who have suffered forms of violence other than OSEC, to call for safer platforms online. The Philippines Survivor Network is one of many chapters of the Global Survivor Network.*

I. Introduction

1.1.1. International Justice Mission (IJM) provides this submission to the Australian government's Statutory Review of the *Online Safety Act 2021* ("OSA"). IJM welcomes this evaluation of the operation of the OSA and the Government's commitment to further strengthening Australia's online safety regime.

1.1.2. International Justice Mission[1] (IJM) is a global organisation that protects people in poverty from violence, partnering with local authorities in 16 countries to combat slavery, violence against women and children, and other forms of abuse. Since 2011, IJM has worked closely with all levels of the Philippine Government, international law enforcement, community service organisations, survivor leaders, and other relevant stakeholders to combat online sexual exploitation of children, with focus on the trafficking of children to produce first-generation child sexual exploitation material (CSEM) especially via livestreamed video ("livestreamed child sexual abuse") in video-chat apps.

Livestreamed child sexual abuse

1.2.1. Livestreamed child sexual abuse is a particularly egregious form of online harm and online child sexual exploitation. Adults around the world pay traffickers or "facilitators" to commit hands-on sexual abuse of often young children while the offenders watch this abuse live online. But the offenders don't just passively watch—they actively direct the assaults and rapes of specific children by typing directives in the chat or audibly on the video call. The offenders and traffickers conspire together to produce new child sexual abuse material that—because it's produced and transmitted in live video—often leaves no digital trace for reporting and investigation. IJM cannot overstate this that these are "live crime scenes" committed daily on common, popular messaging and video-chat applications.[2] See this study report from UK's University of Nottingham Rights Lab, which documented 30 cases beginning in 2010 involving UK offenders using platforms Microsoft Skype, Facebook Messenger, and WhatsApp to livestream child sexual abuse.[3] See also Annex 1 at the end of this Submission for summary descriptions and links to exemplary cases.

1.2.2. It may be tempting to think live video child sexual abuse only happens in the Global South. The reality is that Australian children are victims of child sexual abuse production and distribution via livestreaming. According to the Australian Center to Counter Child Exploitation (ACCCE):

> Australian children *as young as eight* are being coerced into performing live-streamed sexual acts by online predators, who often record and share the videos on the dark net and sexually extort victims into producing even more graphic content.[4]

1.2.3. Increasingly, global law enforcement and experts report the growing threat to children of being sexually abused in live video streamed to offenders globally, with the U.S. Financial Intelligence Unit, FinCEN, reporting a 147% increase in SARs filings related

[1] https://www.ijm.org/

[2] https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse

[3] "Legal and institutional responses to the online sexual exploitation of children," University of Nottingham Rights Lab, September 2023, https://www.nottingham.ac.uk/research/beacons-of-excellence/rights-lab/resources/reports-and-briefings/2023/october/legal-and-institutional-responses-to-the-online-sexual-exploitation-of-children-the-united-kingdom-country-case-study.pdf, page 10.

[4] AFP warn about fast growing online child abuse trend, Sept. 2021, https://www.afp.gov.au/news-media/media-releases/afp-warn-about-fast-growing-online-child-abuse-trend

to child sexual exploitation online.[5] Indeed, livestreamed child sexual abuse is a rapidly increasing global crime, with cases having been identified across dozens of countries, including Romania,[6] Ghana,[7] Thailand,[8] the U.S.,[9] and Colombia.[10]

1.2.4. The Philippines—an Australian ally and regional partner—is considered the global hotspot for this form of online exploitation. A recent study conducted by IJM in partnership with the UK's Nottingham Rights Lab estimated that in 2022 alone **nearly half a million Filipino children were trafficked to produce new child sexual exploitation material, including in livestreams.**[11] That is both shocking and preventable.

1.2.5. This form of online exploitation is fueled by demand from offenders in Western countries – especially Australia - who pay for livestreamed abuse of children. According to the Anti-Money Laundering Council in the Philippines, Australia has consistently ranked the 3rd top source (behind the US and UK) of OSAEC[12] payments flagged as "suspicious transactions" by financial institutions, both in terms of volume and PhP value since 2015.[13]

1.2.6. This does not just indicate threat for children in the Philippines, but a study by Childlight reports that "Men in Australia, UK and USA who report online sexual offending behaviours against children also report being 2 - 3 times more likely to seek sexual contact with children between the ages of 10 – 12 years old if they were certain no one would find out."[14] Similarly, Finnish-based NGO *Protect Children* found that 40% of CSAM offenders report having sought contact with a child after viewing the material.[15]

1.2.7. IJM's comments on this statutory review will be made from the perspective of strengthening the OSA to reduce and mitigate the risk that Australian offenders can use

---

[5] "INTERPOL Report Highlights Impact of COVID-19 on Child Sexual Abuse," INTERPOL, accessed 9 May 2024, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse#:~:text=INTERPOL%20report%20highlights%20impact%20of%20COVID%2D19%20on%20child%20sexual%20abuse; "Internet Organised Crime Threat Assessment (IOCTA) 2020," Europol, accessed 9 May 2024, https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020; "Global Threat Assessment 2021," WeProtect Global Alliance, 19 October 2021, https://www.weprotect.org/global-threat-assessment-21/; "FinCEN Calls Attention to Online Child Sexual Exploitation Crimes," *The Financial Crimes Enforcement Network (FinCEN)*, 16 September 2021, https://www.fincen.gov/sites/default/files/shared/FinCEN%20OCSE%20Notice%20508C.pdf.

[6] https://www.independent.co.uk/news/uk/crime/paedophiles-philippines-romania-national-crime-agency-b2112832.html

[7] https://www.nationalcrimeagency.gov.uk/news/registered-sex-offender-paid-to-watch-live-streamed-child-abuse

[8] DISRUPTING HARM IN THAILAND: Evidence on online child sexual exploitation and abuse, available at https://www.end-violence.org/sites/default/files/2022-02/DH_Thailand_ONLINE_final.pdf, p. 58 ("The victimisation of children via video calls is a common form of OCSEA, according to [the Thailand Internet Crimes Against Children task force] TICAC, and live-streaming of CSEA has appeared in the caseload of DSI. In addition, one foreign law enforcement agency notes that Thailand accounts for 5% of its total reports to date on live-streamed CSEA.")

[9] "UK man jailed for directing the sexual abuse of children around the world," *National Crime Agency*, 25 January 2024, https://www.nationalcrimeagency.gov.uk/news/uk-man-jailed-for-directing-the-sexual-abuse-of-children-around-the-world.

[10] Colombia February 2023 case where police safeguarded three children aged 19 months, seven and nine years, and arrested their mother and aunt accused of livestreaming child sexual abuse for profit, *see* "Horror En Medellín: Madre Obligaba a Sus Tres Hijos de 19 Meses, 7 Y 9 Años a Grabar Pornografía Infantil," *Semana.com*, 27 February 2023, https://www.semana.com/nacion/articulo/horror-en-medellin-madre-obligaba-a-sus-tres-hijos-de-19-meses-7-y-9-anos-a-grabar-pornografia-infantil/202311/.

[11] IJM (2023), *Scale of Harm: Estimating the prevalence of trafficking to produce child sexual exploitation material in the Philippines* https://www.ijm.org.ph/resources

[12] OSAEC – Online Sexual Abuse and Exploitation of Children

[13] http://www.amlc.gov.ph/images/PDFs/Main/Online%20Sexual%20Abuse%20and%20Exploitation%20of%20Children%20in%20the%20Philippines.pdf

[14] https://childlight.org/nature-online-offending-against-children-population-based-data-australia-uk-and-usa

[15] Tech Platforms Used by Online Child Sexual Abuse Offenders, Research Report with Actionable Recommendations for the Tech Industry, *Protect Children*, February 2024.

technology and platforms available in Australia to sexually abuse and exploit both Australian children and children anywhere in the world.

II. Summary of Recommendations

2.1.1. IJM's key recommendation for strengthening Australia's online safety regime is for the development of a substantive duty of care framework to underpin the Online Safety Act ("OSA"), considering the best interests of the child. The OSA should introduce a general and overarching framework of expectations for service providers to develop safe platforms, subsequently outlining specific requirements to prevent illegal content distribution, taking active measures to amend high-risk features and functions of services.

2.1.2. In considering the duty of care, IJM recommends broadening the scope of the Basic Online Safety Expectations to include device manufacturers and companies managing operating systems to adequately capture the nature of online sexual exploitation of children offending and focus on prevention via safety by design.

2.1.3. The duty of care and Basic Online Safety Expectations should be enforceable, with sanctions and penalties in line with online safety regulations in international jurisdictions and in comparable Australian regimes.

2.1.4. IJM's specific recommendations are as follows:

Recommendation 1: Ensure that the provisions of the Act, the Basic Online Safety Expectations Determination and industry codes and standards protect the safety of all users and non-users who are impacted by the use of digital services in Australia, in keeping with the definition of "online safety for Australians" and the stated objectives of the Act.

Recommendation 2: Add as an object of the Act, "*(c) to promote the best interests of the child"* and ensure that this principle is made explicit throughout the Act.

Recommendation 3: Ensure that equipment manufacturers and providers of operating systems are included within the scope of the Basic Online Safety Expectations with specific requirements of safety by design applicable to them.

Recommendation 4: Amend the applicability of the Basic Online Safety Expectations so that all sectors of the digital industry are required to meet online safety expectations.

Recommendation 5: Include as an expectation that camera-enabled devices be built with Child Sexual Abuse Material prevention technology designed to prevent CSAM production, rendering, displaying, distribution, transmission, uploading, and storage.

Recommendation 6: Make the Basic Online Safety Expectations mandatory and enforceable for all digital service providers and invest the eSafety Commissioner with powers to impose penalties for breach of those measures.

Recommendation 7: Create a general duty of care in addition to subsequent detailed requirements for service providers to exercise care in relation to harm caused to or by Australians through the use of their service -

a) to have proportionate measures in place to ensure the online safety of all

persons whose rights are impacted by the use of the service, both users and non-users who experience harm through an Australian's use of the service;

b) to conduct risk assessments of all their systems, features, and functionalities for serious risks they may pose to Australians and by Australians;

c) to conduct a children's safety risk assessment of *all* their services and systems accessible in Australia;

d) to ensure that the best interests of the child are the primary consideration in all actions regarding the provision, regulation, design, management and use of digital technologies accessible in Australia, and to ensure that their services uphold children's right to privacy, safety, dignity and expression, and to protect them from experiencing violence and harm online;

e) to take reasonable steps to mitigate risks identified and report on mitigation measures taken, and to continually assess the effectiveness of those measures and to identify forthcoming plans to strengthen those mitigation measures annually;

f) to develop risk mitigation measures specifically related to child sexual exploitation;

g) to prevent illegal content from entering their platforms accessible to Australians; and

h) to prevent access to illegal content by minor users in Australia.

Recommendation 8: Provide for strong enforcement of the duty of care obligation:

(a) Enable the eSafety Commissioner to enforce civil penalties for failure to comply. The amount of the civil penalty should be in line with penalty amounts available to regulators in other jurisdictions.

(b) Repeal section 235 and create a private right of action against digital service providers for failure to meet the duty of care.

Recommendation 9: Duty of care and online safety obligations should apply equally to all digital services, regardless of the reach of the service or apparent level of risk, to make online safety standards essential to operating in the digital age and remove safe havens for offenders to exploit smaller or seemingly less risky platforms.

Recommendation 10: The eSafety Commissioner should be given powers to order specific action to remedy a breach of the Act or to ensure that a breach is unlikely to recur in the future.

Recommendation 11: Penalty amounts under the Act should be increased to 10% of annual turnover, to be consistent with comparable regimes in Australia and with online safety regulation in international jurisdictions.

Recommendation 12: Provide the Commissioner with powers to impose business disruption measures.

Recommendation 13: Require digital services and platforms who are not making reports of suspected child sexual exploitation and child sexual exploitation material to NCMEC to report suspected child sexual abuse and child sexual abuse material to the Australian Federal Police. Provide the Commissioner with powers to mandate the type of information to be included in the reports and the timeframe for sending those reports. Establish detailed record keeping/content preservation requirements and more appropriate penalties for failure to report content in line with requirements under industry codes and standards.

Recommendation 14: Establish a mechanism within the Act for consulting individuals with lived experience such as survivors of child sexual exploitation or abuse online when developing or amending regulatory frameworks or criminal law provisions related to online child sexual exploitation and abuse.

Recommendation 15: Establish a process of accreditation for safety technologies that can prevent and address child sexual exploitation and child sexual exploitation material and have eSafety maintain a public register of accredited technologies.

Recommendation 16: Bring in amendments to criminal law to provide a pathway for compensation to victims of online sexual exploitation that is easily accessible for domestic and foreign victims and covers medical services such as physical, psychiatric or psychological care, social services, transportation, legal expenses and other relevant losses incurred by the victim.

Recommendation 17: Require digital service providers to undertake risk assessments that identify risk of harm to users generally, specific risk of harm to children and other vulnerable groups, and risks specific to platform functionality. Establish a publicly available register of risks and risk profiles.

Recommendation 18: Australia should introduce an annual cost recovery levy on online service providers that covers the costs for administering the Online Safety Act.

III. Responses to Inquiry Questions

Q1: Are the current objects of the Act to improve and promote online safety for Australians sufficient or should they be expanded?

Ensure clarification and full integration of current Act objectives throughout Australia's online safety regime

3.1.1. The overarching objects of the Act, as set out in section 3 are:

> (a) to improve online safety for Australians; and
> (b) to promote online safety for Australians.

These two objects of the Act are clarified by putting a focus on the capacity of Australians to use electronic services safely, defined as follows:

> online safety for Australians means the capacity of Australians to use social media services and electronic services in a safe manner.

3.1.2. The phrase "capacity of Australians to use … in a safe manner" should be interpreted to include both (i) Australian users being able to use social media and electronic services so that they do not experience harm, and (ii) Australian users being able to use social media and electronic services in such a way that they do not cause harm to others (users and non-users alike). In other words, using a service "safely" not only refers to the safety of the Australian user, but also the safety of anyone who could be harmed by that Australian user's use or misuse of the service.

3.1.3. An individual cannot be said to have the capacity to use a gun safely, for instance, merely because the gun contains safety mitigations to prevent *him* from harming himself, but also because it contains safety mitigations designed to prevent him from harming others by its use. The same can be said for safe use of an automobile.

3.1.4. Governments have for decades required that automobile manufacturers make their cars safe to use by drivers and passengers, and also for the benefit of non-drivers such as pedestrians who could be harmed if car brakes malfunction. For example, the U.S. in 2022 passed a law requiring new passenger vehicles manufactured by 2026 to be equipped with drunk driving prevention technology. Companies are creating an alcohol sensor to detect breath alcohol content and prevent cars from being driven by drivers with alcohol levels above the legal limit. This U.S. drunk driving prevention requirement is in the Infrastructure Investment and Jobs Act (under "Impaired Driving")[16]. The U.S. Department of Transportation is preparing to require alcohol-impaired-driving prevention technology to be installed in all new passenger vehicles.[17]

3.1.5. Essentially, that law requiring prevention technology will give Americans the "capacity to use vehicles in a safe manner," insofar as it relates to potential drunk driving— for the safety of the driver (the "user"), for the safety of others on the road (other "users"), and also for the safety of non-users—passersby, children playing on a playground, children walking home from school, etc.

3.1.6. Likewise, in the OSA, "capacity to use … in a safe manner" should be clarified to include ensuring that all Australians have access to social media and electronic services, including video-chat apps, that have preventative safety technology built in from the start, to make those platforms and services safer by design for users and non-users alike. Why should Australia demand anything less from the technology sector? Why should Australia allow technology companies to build platforms, apps, and services that lack basic safeguards designed to give all Australians the capacity to use them safely?

3.1.7. This topic is critical for Australia's leadership in the digital age. A study by the Australian Institute of Criminology (AIC) found that 256 Australians spent AUD$1.3 million to view live streamed child sexual abuse of Filipino children over a 13-year period.[18] None of these child victims were Australian end-users, yet online platforms and services available in Australia and used by Australians were weaponised for their harm. None of those platforms and services included any technology to allow for Australians to use them 'safely.' Interpreting "capacity to use… in a safe manner" to include preventing harm to non-users—both Australian children and children anywhere—would oblige companies to do something to address this rampant production and streaming of live child sexual abuse by Australian users of vulnerable non-users.

3.1.8. Such an interpretation would make Australia a world-leader but it comes with global underpinnings and support. For example, the World Economic Forum Global Coalition for Digital Safety recently published a paper titled "Making a Difference: How to Measure Digital Safety Effectively to Reduce Risks Online."[19] In it, WEF's Global Coalition of experts from the tech sector, government, online safety regulators, non-profits, and more, call out the need for digital "safety" to include preventing harm to non-users:

> "Online platforms can also be evaluated based on their processes, tools and rules designed to promote the **"safe use" of their services in a manner that mitigates harm to vulnerable non-user groups**."[20]
>
> "Additionally, showcasing strong safety measures promotes trust among users, customers and partners, demonstrating a commitment to protecting online users **while also**

[16] https://www.nhtsa.gov/bipartisan-infrastructure-law

[17] https://www.nhtsa.gov/press-releases/drive-sober-campaign-launch-winter-2023

[18] Brown R. Napier S & Smith R 2020. "Australians who view live streaming of child sexual abuse: an analysis of financial transactions." Trends & issues in crime and criminal justice no. 589. Canberra: Australian Institute of Criminology https://www.aic.gov.au/sites/default/files/2020-05/ti589_australians_who_view_live_streaming_of_child_sexual_abuse.pdf

[19] https://www.weforum.org/publications/making-a-difference-how-to-measure-digital-safety-effectively-to-reduce-risks-online/

[20] Id. at p. 14.

minimizing the risk of harm to nonusers or the public caused by misuse of platforms."[21]

3.1.9. IJM argues that this understanding of the definition of "online safety for Australians" should be reflected throughout the Act, in the Basic Online Safety Expectations Determination and the industry codes and standards to ensure that the focus be on both the safety of users and those whose safety is impacted by others' use of electronic services. This could be done by way of explanatory notes in the legislation, or changes to wording of the text of the provisions.

3.1.10. For example, section 46 of the Act which sets out the core expectations for the BOSE that "...the provider of the service will take reasonable steps to ensure that end-users are able to use the service in a safe manner" should make clear that the expectation refers to the safety of both users and non-users who are impacted by the use of service. Other examples of where the inclusion of safety of non-users can be made explicit are BOSE Determination, sections 6(2A), 6(3)(f) & (j), 14(1).[22]

3.1.11. It is critically important that the OSA regime takes into consideration non-users who are harmed by Australians through the use of services and platforms accessed by Australians in Australia. In some of the worst forms of online child sexual abuse – such as livestreamed child sexual abuse - children who are non-users undergo severe harm and trauma.

3.1.12. In the words of survivor leader Cassie* [*pseudonym*], a survivor exploited and brought to safety in the Philippines:

> *"I was 12 years old when I became a victim of online sexual exploitation. My trafficker would make us an account on the website, a dating app, and change our names and ages there. He posted our pictures on that site so that customers will be attracted and they can chat with me but my trafficker was the one who handled that account using my pictures with a fake name and age."*

When asked "Why do you think it is important that children who are abused on someone else's account should be protected as if they were a registered user themselves?" she replied:

> *"So that innocent children will be protected from someone's account. Technology companies should be aware about this issue and do some action to protect children using social media."*

3.1.13. According to the Internet Watch Foundation's research on livestreamed child sexual abuse, 98% of victims are 13 or under, and forty percent of the livestream captures or recordings were classified as containing 'serious' sexual abuse, *with 18 percent involving the rape and sexual torture of children*.[23] According to a recent study on

---

[21] Id. at p. 5.

[22] BOSE Determination (as amended 29 May 2024)

s. 6(2A) The provider of the service will take reasonable steps to ensure that the best interests of the child are a primary consideration in the design and operation of any service that is likely to be accessed by children.

s. 6(3)(f) assessing whether business decisions will have a significant adverse impact on the ability of end-users to use the service in a safe manner and in such circumstances, appropriately mitigating the impact;

s. 6(3) (j) preparing and publishing regular transparency reports that outline the steps the service is taking to ensure that end-users are able to use the service in a safe manner, including: ...

s. 14(1)(a): The provider of the service will ensure that the service has ... policies and procedures in relation to the safety of end-users...

[23] *See* https://www.iwf.org.uk/news-media/news/iwf-research-on-child-sex-abuse-live-streaming-reveals-98-of-victims-are-13-or-under/; Internet Watch Foundation 2018. Trends in child sexual exploitation: Examining the distribution of captures of live-streamed child sexual abuse. Cambridge, UK: Internet Watch Foundation. https:// www.iwf.org.uk/resources/research

prevalence of online perpetration, 1.7% of Australian adult men have paid for online sexual interactions, images or videos involving a person under 18.[24]

3.1.14. Despite the clear definition of "online safety for Australians" in the Act, the BOSE and industry codes and draft standards have focused only on the safety of *end-users*. Our online safety regime should ensure that Australia's regulation of the online environment also protects *non-users who are harmed through the misuse of services and platforms operating in Australia by Australians*.

Preventing users from engaging in harmful online behaviour:

3.1.15. Ensuring offenders cannot harm children online not only protects children, but it also protects Australians from encountering harmful content online that could lead them down the pathway to child sexual abuse offending.

3.1.16. Elly Hanson, psychologist, presented evidence from numerous studies at the 2024 PIER24 conference looking at how online pornography contributes to pathways to child sexual abuse.[25] Research indicates that pornography can lead people to view child sexual abuse material (and all this can flow into other forms of child sexual abuse), and it increases the risk of child sex abusers re-offending.

3.1.17. For example, analysis of qualitative data in a CSAM dark web survey by Finnish NGO Protect Children revealed that respondents may begin searching for CSAM when they are "bored," "unexcited" or "tired" of adult pornography.[26] Further, WeProtect Global Alliance's 2023 Global Threat Assessment found that:

> "possible links between regular viewing of pornography and the likelihood of suffering or perpetrating child sexual exploitation and abuse online — not least because young people themselves recognise the negative impacts of exposure to online pornography.

3.1.18. In a survey[27] of young New Zealanders carried out in 2020, most called for steps to be taken by online service providers and governments to restrict access to pornographic and extreme sexual content online."[28]

3.1.19. Separately, Michael Sheath, principal practitioner at the Lucy Faithfull Foundation and a counsellor with 33 years of experience working with men who abuse children, has found a link between the extreme nature of internet pornography and deviant or criminal behaviour. Speaking to the Guardian about the men he has worked with, he said:

> "…mainstream pornography sites are changing the thresholds of what is normal and I think it's dangerous […] If you look at the videos on mainstream porn sites you can see 'teen' themes, 'mom and son' themes, lots of incestuous porn. It's pretty deviant stuff. To watch this you have already lowered your threshold of what is acceptable. Porn is an entry drug for a lot of them."[29]

3.1.20. The Online Safety Act needs an appropriate response to protect children and non-users *from* Australian offenders and a regime with requirements designed to prevent Australians *from experiencing content that is harmful to the users themselves.*

---

[24] Childlight (2024), *Into the Light: Childlight global index of child sexual exploitation and abuse prevalence*. https://childlight.org/sites/default/files/2024-05/into-the-light.pdf

[25] https://www.youtube.com/watch?v=vlPoUur05Yw

[26] https://suojellaanlapsia.fi/en/post/redirection-blog-02-russian-speaking-csam-users

[27] https://www.classificationoffice.govt.nz/resources/

[28] https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf

[29] https://www.theguardian.com/global-development/2020/dec/15/how-extreme-porn-has-become-a-gateway-drug-into-child-abuse

Recommendation 1: Ensure that the provisions of the Act, the Basic Online Safety Expectations Determination and industry codes and standards protect the safety of all users and non-users who are impacted by the use of digital services in Australia, in keeping with the definition of "online safety for Australians" and the stated objectives of the Act.

Expand the objects of the Act

3.2.1. The current objects of the Act should be expanded to include an additional object, *"to promote and protect the best interests of the child."* This would be consistent with the recent amendment to the BOSE Determination that puts an expectation on tech companies to take reasonable steps to ensure that the best interests of the child are a primary consideration throughout the development and implementation of a digital service [s. 6(2A)]. Explicitly making the best interests of the child an object of the Act itself would reinforce the importance of the best interests of the child and place it as an overarching consideration throughout every aspect of the provision, design, regulation, management and use of digital services. [30]

3.2.2. Setting the best interests of the child as an object would also improve and promote the online safety of ***all*** children – the digital environment plays a significant role in children's lives, affecting them in various ways regardless of whether they are users of digital services. As stated in the UN Committee on the Rights of the Child (UNCRC) in their General Comment on children's rights in relations to the digital environment,

> the rights of every child must be respected, protected and fulfilled in the digital environment. Innovations in digital technologies affect children's lives and their rights in ways that are wide-ranging and interdependent, *even where children do not themselves access the Internet [emphasis added].*[31]

3.2.3. In the case of livestreamed child sexual abuse, children experience repeated hands-on sexual abuse at the hands of a trusted adult, which is livestreamed to paying sex offenders around the world, including Australians. Many of the child victims are not end-users of the digital platforms through which the abuse occurred but they are harmed by users accessing those platforms from Australia.

3.2.4. Further, including "best interest of the child" as an object of the Act acknowledges the borderless nature of the digital environment and ensures that online safety protections extend beyond Australian end-users, where there is an Australian nexus. The safety risks and impacts of internet misuse on Australian platforms are not confined to end-users in Australia; many Australians are involved in exploiting and causing online harm to others outside of Australia. The Philippines found that Australians accounted for nearly 1 in 5 offenders who engage in livestreamed sexual abuse of children in the Philippines. None of the child victims were Australian end-users, yet online platforms available in, and used by Australians, were weaponised for that harm.

Recommendation 2: Add as an object of the Act, *"(c) to promote the best interests of the child"* and ensure that this principle is made explicit throughout the Act.

Q2: Should the Act have strengthened and enforceable Basic Online Safety Expectations?

4.1 IJM has the following recommendations for strengthening the Basic Online Safety

[30] See General comment No. 25 (2021) on children's rights in relation to the digital environment | OHCHR, para. 12.

[31] General comment No. 25 (2021) on children's rights in relation to the digital environment | OHCHR, para. 4

Expectations under the Act.

Expand the Scope of the BOSE

4.1.1. Currently the Basic Online Safety Expectations apply to only three sections of the online industry – Social Media Services (SMS), Relevant Electronic Services (RES) and Designated Internet Services (DIS). However, service providers within the whole of the digital industry should be expected to take reasonable steps to ensure online safety for users and those impacted by the use of online platforms.

4.1.2. For example, equipment manufacturers and providers of operating services (*ie* those service providers covered by the Equipment Industry Code) have the ability to incorporate safety into the design and engineering of devices, and control the engineering decisions related to the features and settings made available to end-users by way of the operating system of the device. As social media services and other electronic services are accessed by devices and run on operating systems, embedding technology to facilitate 'Australian's safe use of" social media and electronic services, online safety and prevention of online harms at the level of the device or operating system provides protection regardless of the platform or app being used.

4.1.3. Placing Basic Online Safety Expectations on equipment providers and relevant operating systems (iOS and Android) to design the equipment and run operating systems safe by design ensures scaling of online safety and keeping up with the changing online environment as new apps and platforms come online daily. For example, building in technology designed to prevent and disrupt the production and sharing of child sexual abuse material (CSAM) at the OS or device level would ensure devices and operating systems are "safe by design" to prevent CSAM from being produced, uploaded or shared, regardless of the new apps being used that may not have such safety features. And the leading device manufacturers and OS managers—Apple, Google, and Microsoft—have no shortage of resources to dedicate to building and deploying such CSAM prevention technology to the benefit of Australian users, including children, regardless of which website or app they use.

4.1.4. Moreover, CSAM prevention technology embedded on devices and via operating systems supports efforts to balance child protection with user privacy and data privacy. Big tech companies themselves attest to this.

4.1.5. For instance, Apples explains that because content is analysed on device, it is protective of user privacy:

> Communications Safety uses on-device machine learning to analyze photo and video attachments and determine if a photo or video appears to contain nudity. Because the photos and videos are analyzed on your child's device, **Apple doesn't receive an indication that nudity was detected and doesn't get access to the photos or videos as a result.**

4.1.6. WhatsApp similarly explains:

> WhatsApp automatically performs checks to determine if a file is suspicious, to ensure that the format is supported on WhatsApp and doesn't crash the app on your device. **To protect your privacy, these checks take place entirely on your device and because of end-to-end encryption, WhatsApp can't see the content of your messages.**

4.1.7. Requiring this technology to move up the tech stack to device manufacturers / operating systems effectively scales its impact across whatever app, platform or website is being used on the device. That is why the government of Australia should require that camera-enabled devices come installed with safety features and technology designed to prevent

the capture and rendering of CSAM, among other safety mitigations.

4.1.8. Similar to a recently passed bill in the United States that requires auto-manufacturers to build into every vehicle drunk driving prevention technology that prevents intoxicated drivers from operating vehicles, camera-enabled devices should come installed with CSAM prevention technology – to make them safe by design and unable to record, capture, or render child sexual abuse and exploitation. To provide some concrete examples of what safety by design requirements for device manufacturers and operating system companies could potentially look like, *see* Annex II for a proposed policy brief with potential relevant language to be adapted to relevant legal frameworks.

4.1.9. One such example of technology that can be installed on device at the operating system level is SafeToNet's HarmBlock. This technology can integrate into device operating systems for all device manufacturers, making their products inherently safe by rejecting harmful or illegal sexual content.[32]

Recommendation 3: Ensure that equipment manufacturers and providers of operating systems are included within the scope of the Basic Online Safety Expectations with specific requirements for safety by design applicable to them.

Recommendation 4: Amend the applicability of the Basic Online Safety Expectations so that all sectors of the digital industry are required to meet online safety expectations.

Recommendation 5: Include as an expectation that camera-enabled devices be built with Child Sexual Abuse Material prevention technology designed to prevent CSAM production, rendering, displaying, distribution, transmission, uploading, and storage.

Basic Online Safety Expectations should be enforceable

4.2.1. The Basic Online Safety Expectations have been effective in providing greater transparency on what tech companies are and are not doing to address CSAM and online child sexual exploitation, and hence in disclosing gaps and further steps that need to be taken to ensure greater protection for children. The exercise of the eSafety Commissioner's powers to compel companies to answer questions on steps they are taking to address child sexual exploitation found that there are serious shortcomings and differences in the use of technological tools, policies, and rules to detect, report, and prevent child abuse material and grooming.

4.2.2. Despite the expectation under BOSE, section 6(2) of service providers taking "reasonable steps to proactively minimise the extent to which material or activity on the service is lawful or harmful", the eSafety Commissioner's reports[33] revealed that some companies were not using available technology to identify and minimise child sexual exploitation material and activity. For example, some companies did not attempt to proactively detect child abuse material stored in cloud services, despite the wide availability of PhotoDNA detection technology. Also, despite the availability of databases that identify URLs hosting known child sexual exploitation and abuse

[32] https://safetonet.com/

[33] Basic Online Safety Expectations: Summary of industry responses to the first mandatory transparency notices, December 2022 https://www.esafety.gov.au/sites/default/files/2022-12/BOSE%20transparency%20report%20Dec%202022.pdf?v=1718052520879; Basic Online Safety Expectations: Summary of industry response to mandatory transparency notices, October 2023 https://www.esafety.gov.au/sites/default/files/2024-03/Basic-Online-Safety-Expectations-Non-Periodic-Notices-Issued-February-2023_0.pdf?v=1718052520878.

material (CSEA) and websites that are dedicated to it, some companies are not using them.

4.2.3. Further, according to the eSafety Commissioner's first report, "eSafety's understanding from their responses to the notice questions is that the providers are neither taking action to detect CSEA in livestreams (insofar as any of these could be regarded as livestreaming services) or taking action to detect CSEA in video calls or conferences."[34]

> *"In my experience, I became a victim at age 10 and I was rescued at age 17, so I experienced trauma for more than 5 years. If when I was a victim, tech companies used detection tools, I would not have suffered for so many years and there wouldn't be other victims of my perpetrator." (Joy*)*

4.2.4. In allowing the regulator to exercise discretion in asking specific targeted questions, the BOSE provisions enable disclosure of meaningful information and the ability to keep pace with the rapidly changing digital environment. Increased transparency is helpful, but it does not necessarily lead to action by tech companies to improve online safety measures. The eSafety Commissioner lacks powers to hold digital services providers accountable for failing to meet expectations under BOSE to take reasonable steps to minimise online harm. Voluntary standards, where the consequence of a breach is merely reputational damage, have little to incentivise tech companies to adequately protect users.

4.2.5. As noted in the Issues Paper, other jurisdictions have opted for mandatory/enforceable standards. Under the EU's Digital Services Act and the UK's Online Safety Act, regulators have the power to compel platforms to change and improve safety standards and to issue significant fines for failure to adequately mitigate safety risks. [See below for discussion on enforcement more generally.] The UK and EU regulators also allow, in extreme cases, to order the restriction of access to the service provider. The UK legislation also provides for imposition of criminal sanctions on senior directors if they fail to produce material requested by the regulator.

4.2.6. IJM recommends, in keeping with the global trend in regulating digital spaces, that the Basic Online Safety Expectations be enforceable, through significant monetary penalties for breaches of measures set out in the expectations and the ability of the regulator to compel particular action/steps.

> **Recommendation 6**: Make the Basic Online Safety Expectations mandatory for all digital service providers and invest the eSafety Commissioner with powers to impose penalties for breach of those measures.

Service providers should be expected to comprehensively address safety risks of their systems

4.3.1. Australia's current regulatory regime takes a hybrid approach to addressing online safety, providing an individual complaints mechanism about specific types of online content, while also placing systemic requirements on digital platforms through reasonable steps under the BOSE that service providers are expected to take with respect to more systemic safety risks. The recent amendments to the BOSE include additional expectations to reflect emerging trends and issues in digital spaces, such as generative

[34] https://www.esafety.gov.au/sites/default/files/2022-12/BOSE%20transparency%20report%20Dec%202022.pdf at p. 15

AI. This points to the issue that an evolving online environment will always leave gaps that are left unregulated. These gaps and the BOSE expectations in general can be strengthened by a statutory duty of care framework, in line with the approach of the UK, Ireland and the proposed Canadian legislation.

4.3.2. It is important that service providers comprehensively address safety risks of their systems. As pointed out in the Report of the House of Representatives Select Committee on Social Media and Online Safety,[35] the use of a **statutory duty of care** would ensure that service providers take responsibility for creating systems which are protective of users. It flips the onus to provide and ensure user safety back on the service providers. A duty of care framework would assist in ensuring that digital service providers "have an incentive to create systems, and improve current ones, to ensure the safety of all users, particularly children, women and other vulnerable groups. A formalised duty of care would also ensure that such a model incorporates penalties for noncompliance."[36]

Incentivising service providers

4.4.1. A duty of care approach shifts the burden of online safety away from the users and onto the entities who have control, expertise and resources, and who are responsible for allowing a hazardous digital environment. The eSafety Commissioner has been working with technology companies to promote and support a **Safety by Design** approach to the development of products and services, to minimise online threats by anticipating and eliminating online harms *before* they occur. The BOSE also contains expectations related to Safety by Design [37] ; however, those expectations lack enforceability. Mandating a general duty of care incentivises digital service providers to build in safety, from the get-go, into the design, development and deployment of products and services to prevent online harms before they occur, while also enabling providers flexibility to develop varying approaches to ensure online safety according to the functions and features of the platforms and services in question.

4.4.2. This outcomes-based approach (ie harm prevention) creates incentive for service providers to invest in proactive risk assessments and mitigations. As they would be held responsible for harms materialising from any reasonably foreseeable risks, they would be incentivised to deploy resources to identify and manage those risks.

A general duty of care in relation to online harms

4.5.1. IJM recommends that the Act establish a general, overarching obligation for service providers to exercise care in relation to harm caused through the use of their service followed by more granular expectations. The general duty would consist of a requirement to have proportionate measures in place to ensure the online safety of all persons whose rights are impacted by the use of the service, both users and non-users who experience harm through another user's use of the service. This approach looks beyond harmful content on the platforms and requires service providers to look at whether there is risk of harm to their users (and others who are impacted by end-users using the platform) arising from the service or platform's technical systems, design, rules, policies, and business models.

4.5.2. The UK's draft Illegal Harms Codes of Practice illustrates this well. In its development

[35] Parliament of Australia, *Social Media and Online Safety* (March 2022) https://parlinfo.aph.gov.au/parlInfo/download/committees/reportrep/024877/toc_pdf/SocialMediaandOnlineSafety.pdf;fileType=application%2Fpdf

[36] Committee Report at paragraph 5.83.

[37] BOSE s. 6(3)(a): ensuring that assessments of safety risks and impacts are undertaken, and safety review processes are implemented, through the design, development, deployment and post-deployment stages for the services.

of a risk register, it includes all of the features and functionalities that a platform may have that could lead to sexual exploitation of children. It includes functionalities like livestreaming, private messaging, virality capabilities, end-to-end encryption, and many others. This demonstrates that many major platforms have features that increase the risk of their platforms being misused to sexually abuse and exploit children without mitigation or prevention measures, and with minimal accountability for offending users.

4.5.3. The UK Online Safety Act also expressly defines the duty of care for platforms to include the removal of illegal content, prevention of illegal content distribution, risk mitigation related to child sexual exploitation, the prevention of children from accessing harmful and age-inappropriate content, as well as assessing the features and functionalities of a service for potential harm.

4.5.4. The following obligations under the duty of care should be explicitly set out within the Act:

4.5.5. *Risk assessment requirement:* A statutory duty of care approach would require service providers to conduct risk assessments of all their systems, features, and functionalities for serious risks they may pose. Consider the UK's Ofcom risk register as a mechanism for harmonisation of regulatory regimes. The risk assessment should be undertaken annually and whenever there is a significant change to the features of the platform. The risk assessment should be submitted to the eSafety Commissioner, and, to the extent deemed safe and appropriate by eSafety, made available publicly.

4.5.6. *Mitigation measures:* As part of a risk assessment, the duty of care obligation would require service providers to take reasonable steps to mitigate each of the risks identified and to report on those measures taken. The requirement for mitigation would include an obligation to continually assess the effectiveness of those measures and to identify forthcoming plans to strengthen those mitigation measures annually.

4.5.7. *Enforceability:* The duty of care should be enforceable by the regulator with strong penalties for failure to comply. Furthermore, individuals should have a private right of action against tech companies for failure to comply. A counter-example from the U.S. is section 230[38] of the Communications Decency Act of 1996 which is seen as one of the great hinderances to tech accountability.[39] This section provides blanket immunity to online computer services specific to any third-party content generated, uploaded, or circulated by its users. Many experts[40] in the field are calling for section 230 to be repealed so that tech companies can be held liable for illegal content or conduct on their platform, and therefore incentivise companies to establish prevention mechanisms for the production and distribution of illegal content on their services.

Duty of care and the best interests of the child

4.6.1. Children's lives and well-being are profoundly impacted by the digital environment. Recent research on the global scale and prevalence of child sexual exploitation and abuse found that more than 300 million children a year are victims of online sexual abuse and exploitation.[41] The same study found that 11% of men in the United States, 7% of men in the UK and 7.5% of men in Australia report that they have engaged in online behaviours at some point in their lifetime that could be classed as online child sexual abuse

[38] https://crsreports.congress.gov/product/pdf/R/R46751

[39] https://www.judiciary.senate.gov/press/dem/releases/durbin-delivers-opening-statement-during-judiciary-subcommittee-hearing-on-social-media-platform-accountability-and-opportunities-for-reform

[40] https://www.brookings.edu/articles/section-230-reform-deserves-careful-and-focused-consideration/

[41] *Into the Light: Childlight global index of child sexual exploitation and abuse prevalence*, Childlight, 2024. into-the-light.pdf (childlight.org)

offending.

4.6.2. A general duty of care to prevent online harm, as it relates to children, must be based on the principle of the best interest of the child. As recommended by various submissions to the House of Representatives Committee on Socia Media and Online Safety, the best interest of the child must be a foremost consideration in all action that affect children in the public and private spheres, including all actions regarding the provision, regulation, design, management and use of digital technologies.

4.6.3. Digital service providers must be held accountable for ensuring that their services uphold children's right to privacy, safety, dignity and expression (as set out in the UN Convention on the Rights of the Child), and protect them from experiencing violence and harm online. These rights of children should outweigh the commercial interests of digital service providers.

4.6.4. A duty of care on service providers to ensure that the design or operation of their online services do not violate children's right to freedom from violence online is articulated as follows in General Comment No. 25 to the UNCRC

> *37. States parties have a duty to protect children from infringements of their rights by business enterprises, including the right to be protected from all forms of violence in the digital environment. Although businesses may not be directly involved in perpetrating harmful acts, they can cause or contribute to violations of children's right to freedom from violence, including through the design and operation of digital services. States parties should put in place, monitor and enforce laws and regulations aimed at preventing violations of the right to protection from violence, as well as those aimed at investigating, adjudicating on and redressing violations as they occur in relation to the digital environment.*[42]

4.6.5. At a minimum, the duty of care with respect to children would require digital service providers to conduct a children's risk assessment (as in the UK & EU) of all their services and systems and to build in risk mitigation measures to protect the rights and online safety of children. The recent amendments to the BOSE include child safety risk assessments as a reasonable step for meeting the expectation of ensuring safe use. As part of an overarching duty of care placed on service providers, a child safety risk assessment should be a core enforceable obligation on service providers.

4.6.6. The eSafety Commissioner should be tasked with monitoring and enforcement of the risk assessments and measures, with sufficient staffing and resources.

<u>Duty of care requires mitigating harm for non-users</u>

4.7.1. A duty of care includes the responsibility to minimise the risk of harm to the public and non-users caused by misuse of platforms. We must recognise that those who suffer online violence and harm from use of digital services are not confined to users of those services. In IJM's experience with cases of livestreamed child sexual abuse, many of the victims who suffer devastating abuse are very young – some as young as two months old – too young to be digital users.

4.7.2. As noted earlier in discussing the objects of the Act, the definition of "online safety for Australians" in the Act refers to capacity to use electronic services safely. "Capacity to use … in a safe manner" includes ensuring that digital systems, platforms and devices are designed and operate in such a way as to prevent their use in a dangerous manner

[42] General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25 (2 March 2021) https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

that causes online harm. Using a service safely not only refers to the safety of the user, but also the safety of anyone who could be harmed by that user's use of the service.

4.7.3. A duty of care approach based on the best interests of the child principle would place a clear onus on digital service providers to ensure protection for all children, both users and non-users. This approach is reflected in a recent report from the World Economic Forum (WEF) Global Coalition on Digital Safety:

> *"Additionally, showcasing strong safety measures promotes trust among users, customers and partners, demonstrating a commitment to protecting online users while also minimizing the risk of harm to nonusers or the public caused by misuse of platforms."*
>
> *"Online platforms can also be evaluated based on their processes, tools and rules designed to promote the "safe use" of their services in a manner that mitigates harm to vulnerable non-user groups."*

Recommendation 7: Create a general duty of care in addition to subsequent detailed requirements for service providers to exercise care in relation to harm caused to or by Australians through the use of their service -

(a) to have proportionate measures in place to ensure the online safety of all persons whose rights are impacted by the use of the service, both users and non-users who experience harm through an Australian's use of the service;

(b) to conduct risk assessments of all their systems, features, and functionalities for serious risks they may pose to Australians and by Australians;

(c) to conduct a children's safety risk assessment of *all* their services and systems accessible in Australia;

(d) to ensure that the best interests of the child are the primary consideration in all actions regarding the provision, regulation, design, management and use of digital technologies accessible in Australia, and to ensure that their services uphold children's rights to privacy, safety, dignity and expression, and to protect them from experiencing violence and harm online;

(e) to take reasonable steps to mitigate risks identified and report on mitigation measures taken, to continually assess the effectiveness of those measures, and to identify forthcoming plans to strengthen those mitigation measures annually;

(f) to develop risk mitigation measures specifically related to child sexual exploitation;

(g) to prevent illegal content from entering their platforms accessible to Australians; and

(h) to prevent access to illegal content by minor users in Australia.

Recommendation 8: Provide for strong enforcement of the duty of care obligation:

(a) Enable the eSafety Commissioner to enforce civil penalties for failure to comply. The amount of the civil penalty should be in line with penalty amounts available to regulators in other jurisdictions.

(b) Repeal section 235 and create a private right of action against digital service providers for failure to meet the duty of care.

Q7 Should regulatory obligations depend on a service provider's risk or reach?

5.1.1. IJM recommends that regulatory obligations apply to service providers generally, and that no differentiation be made based on the provider's reach or risk. Complying with requirements to promote and protect online safety should be a basic requirement for

online services, similar to paying for security or their internet bill. Online safety is not a luxury, but is instead a necessity for any digital service provider wishing to operate its business in Australia. All food service organisations in Australia, for instance, are required to comply with the Food Standards Code, whether they are a large fast-food chain or a mom-and-pop restaurant. All automobiles are required to have built-in safety features, not exempting smaller auto manufacturers. Minimum standards for online safety should be a cost of doing business, and companies should not be allowed to neglect online safety until they are large enough to be causing massive harm to people.

5.1.2. With respect to a service provider's reach, services used by a small percentage of the Australian population might be a niche service used primarily by offenders. Offenders may exploit less developed or smaller online services to evade detection, as these platforms are less likely to deploy robust CSAM detection or prevention technologies. If smaller services were excluded from certain regulatory obligations of the Act, offenders could be enabled to use smaller companies to exploit children where no one is looking.

5.1.3. Concerns may be raised that smaller platforms may not have capacity to deploy certain technological solutions due to lack of financial resourcing; however, many of the technologies are available free of charge or for low cost. For example, the following tools are available without charge:

- Microsoft's PhotoDNA
- NCMEC's Hash Sharing
- Google Content Safety API and CSAI

5.1.4. Other tools are available for low cost. For example, the monthly cost of DragonflAI,[43] for 500,000 active users is approximately $2,290 AUD. For Thorn's Safer tool,[44] a 12-month subscription based on 1M queries per month is $46,081.23 AUD.

5.1.5. Another avenue by which to address the regulatory burden on, and capacity concerns of, smaller platforms is to ensure that equipment manufacturers and OS operators are required to design equipment and run operating systems safe by design so as to prevent CSAM from being produced, uploaded or shared on the equipment or operating system, as set out in Recommendation 3. This would address the challenge of every individual app or platform needing to implement their own safety technology, but instead allow implementation of preventative technology at scale, through the device and/or operating system. *[See discussion above at paras. 4.1.2, 4.1.3, 4.1.7]*

5.1.6. Similarly, seemingly less risky services should have the same responsibilities for online protection as those that are perceived to have higher risk. There have also been recent instances of sextortion offenders meeting children on larger platforms but moving to smaller ones to continue the exploitation. As part of the extortion and account takeover, they take over the child's school account and extort all of the other children within the platform. It is a cross-platform issue, and smart offenders are using these small platforms to get into the child's closer network. This has been seen specifically in school communication platforms. Even services that would assumably be less risky should deploy safety technology to prevent child exploitation.

5.1.7. Consequently, it is imperative that even smaller or seemingly less risky companies adhere to every measure outlined in the Codes, ensuring an indiscriminate application of safety protocols. Given the diverse range of platforms available for offenders to exploit

[43] AUD equivalent of £1200.12 GBP, https://www.dragonflai.co/pricing

[44] AUD equivalent of $30,720 USD, https://aws.amazon.com/marketplace/pp/prodview-dfwekn4bx4akehttps://aws.amazon.com/marketplace/pp/prodview-dfwekn4bx4ake

children on, coupled with their increasing creativity in conducting that exploitation, it becomes crucial for companies to adopt comprehensive prevention measures.

Recommendation 9: Duty of care and online safety obligations should apply equally to all digital services, regardless of the reach of the service or apparent level of risk, to make online safety standards essential to operating in the digital age and remove safe havens for offenders to exploit smaller or seemingly less risky platforms.

Q17: Does the Act need stronger investigation, information gathering and enforcement powers?

6.1.1. As noted in the Issues Paper, the eSafety Commissioner has powers to require transparency reporting in relation to BOSE expectations, investigate complaints or suspected breaches of industry codes and standards, and to obtain information relating to the identity and contact details of an end-user of social media service, relevant electronic service or designated internet service. Investigative powers include the powers to summon a person to attend before the Commissioner to answer questions or produce documents, require a person to provide information or documents, and examine a person under oath or affirmation. Non-compliance with a requirement to give evidence or produce documents is subject to a civil penalty of 100 penalty units and/or imprisonment for 12 months.

6.1.2. Transparency notices issued to tech companies under the BOSE have revealed what companies currently are doing to address child sexual exploitation and pro-terror material on their services; however, transparency reporting has not been effective in addressing the gaps or compelling changes to corporate practice of tech companies so as to improve online safety for children and all Australians. The Act provides for penalties for non-compliance with a transparency notice or a breach of the codes and standards, but the eSafety Commissioner lacks the power to require companies to take specific measures.

6.1.3. Under the UK's Online Safety Act[45], the regulator is empowered to compel redress to ensure platforms change and improve safety standards. Significant fines attach for failure to do so. Similar provisions empowering the regulator to order corrective action are found in Ireland's Online Safety and Media Regulation Act 2022[46], and Canada's draft Online Harms Bill similarly empowers the regulator to order corrective action where there is a breach/non-compliance.[47] In the Australian context, clause 16 of the exposure draft Communications Legislation Amendment (Combatting Disinformation and Misinformation) Bill 2023[48] provides for the regulator to issue directions to take specific corrective measures.

6.1.4. We recommend that the eSafety Commissioner be empowered to issue remedial direction, requiring the person or entity to take specified action to remedy the breach and/or to ensure that it is unlikely to recur in the future.

Recommendation 10: The eSafety Commissioner should be given powers to order specific action to remedy a breach of the Act or to ensure that a breach is unlikely to

[45] https://www.legislation.gov.uk/ukpga/2023/50/part/7/chapter/6/crossheading/penalty-notices-etc/enacted Section 139-144, UK Online Safety Act of 2023

[46] Section 139ZM. https://www.irishstatutebook.ie/eli/2022/act/41/section/47/enacted/en/html#sec47

[47] Bill C-63, section 94

[48] https://www.infrastructure.gov.au/sites/default/files/documents/communications-legislation-amendment-combatting-misinformation-and-disinformation-bill2023-june2023.pdf

recur in the future.

Q18: Are Australia's penalties adequate and if not, what forms should they take?

7.1.1. Effective enforcement of the Act is essential to preventing online harms and ensuring that the internet is a safe place for everyone.

7.1.2. Under the current framework, the penalties that attach to a breach of the obligations under the OSA are significantly out of alignment with other jurisdictions. The low penalties that attach to non-compliance - a maximum of 2500 penalty points ($782,500) - belie the seriousness of the impact of the online harms caused by non-compliance with safety regulations, especially to the most vulnerable, such as children. Where the fines are lower than the cost of implementing meaningful safety measures to address the breach, there is little incentive for platforms to change and improve safety standards.

7.1.3. By contrast, under the EU's Digital Safety Act (DSA), penalties can be up to 6% of a company's global annual turnover.[49] Other jurisdictions provide for similar level of penalties, ranging up to 10% of global annual turnover or £18M under the UK's OSA[50]; and €20M or 10% of annual turnover under Ireland's Online Safety and Media Regulation Act.[51]

7.1.4. Australia's regulatory framework raises questions as to whether there is adequate deterrence for digital service providers to comply with the requirements under the Online Safety Act. Currently, the consequences of non-compliance are far too weak. Penalties for breaches of online safety requirements cannot be seen as simply a cost of doing business. Service providers must be incentivised to have strong safeguards in place to protect Australian users, Australian children, and other vulnerable populations from online harm.

7.1.5. Penalties under the OSA should be set at levels consistent not only to other jurisdictions but also to other comparable regimes in Australia, such as the penalty schemes under the *Australian Securities and Investment Commissions Act*, *Corporations Act*, *Anti-Money Laundering & Terrorist Finance Act*, and the *Competition and Consumer Act*.[52]

7.1.6. The *Privacy Act 1988* was amended in December 2022 to raise penalties for serious or repeated interferences with privacy from $2.22 million to an amount greater of $50 million, three times the value of benefit obtained or 30% of an entity's adjusted turnover. The rationale for the significant increase in penalty was to incentivise entities to comply with their obligations and to reflect the very serious harms that can result from breaches of those obligations. The same holds true that the penalties under the *Online Safety Act* need to reflect the very serious harms that can result from non-compliance with online safety obligations under the Act. Setting penalties at a higher level will accord with Australian community expectations about the importance of protecting children and adults from online harm. We recommend that penalty amounts under the Act be increased to 10% of annual turnover, to be in line with comparable regimes in Australia

[49] https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement#:~:text=or%20allowing%20inspection.-,Sanctioning%20powers,to%20comply%20with%20interim%20measures

[50] https://www.legislation.gov.uk/ukpga/2023/50/section/72 (Section 72)

[51] https://www.irishstatutebook.ie/eli/2022/act/41/section/47/enacted/en/html#sec47

[52] See Table 4.2 in Issues Paper which sets out penalties for Australian Consumer Law, Privacy Act 1988 and Anti-Money Laundering and Counter-Terrorism Financing Act 2006. Under the Corporations Act and the Australian Securities and Investment Commissions Act, maximum penalties are the greater of 50,000 penalty units ($15.7M), three times the benefit obtained or 10% of annual turnover, capped at 2.5M penalty units.

and consistent with online safety regulation in international jurisdictions.

Recommendation 11: Penalty amounts under the Act should be increased to 10% of annual turnover, to be consistent with comparable regimes in Australia and with online safety regulation in international jurisdictions.

Q20 Should the Commissioner have powers to impose sanctions such as business disruption sanctions?

8.1.1. The Commissioner should have additional tools to enforce action against non-compliance, especially with respect to service providers based overseas. Similar to the provisions in the UK Online Safety Act,[53] Australia's regulator should have the power to impose business disruption measures in situations where other enforcement action (such as fines) do not have the intended effect and the non-compliant action by the service provider continues. Investing the eSafety Commissioner with the ability to require payment providers, advertisers and internet service providers to stop working with the non-compliant services would prevent those non-compliant services from generating revenue in Australia or being accessed from Australia or by Australians when they are wilfully non-compliant with Australian laws and regulations.

8.1.2. We recommend that the Act empower the Commissioner to apply to the Federal Court for a **service restriction order** that would require providers of ancillary services to withdraw services from a non-compliant service provider. The ancillary service provider that is issued the order would be required to take steps to disrupt the business or revenues of the non-compliant provider in Australia, for example by withdrawing payment processing services or ad services to the non-compliant service provider.

8.1.3. Such business disruption orders should be available as an exceptional measure, where the service provider has failed to comply with a requirement or notice under the Act and the non-compliant conduct continues; or the provider has failed to pay a penalty imposed for non-compliance with an obligation under the Act; or there is significant risk of harm to individuals in Australia because of the failure to comply.

8.1.4. Such measures have clear precedent in the offline world. When two Boeing 737 Max planes fell from the sky, leading to catastrophic accidents for the hundreds of passengers on board, governments quickly grounded those planes for 20 months until the defects were addressed.[54] Similarly, Australia's Department of Infrastructure, Transport, Regional Development, Communications and the Arts states the following on its website in describing its product recall powers:

> Vehicle and component recalls are a critical part of keeping you and the vehicles on our roads safe. A vehicle or component recall can occur if there is a safety issue that may cause injury or if the vehicle or component does not comply with applicable standards.[55]

8.1.5. The Australian government should have the same powers to prevent the continued operation of digital platforms and apps in Australia in order to keep Australians and the apps/platforms in Australia's digital environment safe and compliant with applicable standards.

[53] See sections 144-147, *Online Safety Act (UK)* and draft Guidance, volume 6 "Protecting people from illegal harms online" https://www.ofcom.org.uk/__data/assets/pdf_file/0026/271169/annex-11-illegal-harms-consultation.pdf

[54] https://www.independent.co.uk/travel/news-and-advice/boeing-737-max-safety-aircraft-passengers-crash-b2564661.html

[55] https://www.infrastructure.gov.au/infrastructure-transport-vehicles/vehicles/vehicle-recalls

Recommendation 12: Provide the Commissioner with powers to impose business disruption measures.

Q21: Should the Act incorporate any of the international approaches? What should they look like?

Q22 Should Australia place additional statutory duties on online services to make online services safer and minimise harm?

9.1.1. Australia's Act can be further strengthened by incorporating the following features from international approaches to make online services safer and minimise harm.

1) Duty of Care

9.1.2. IJM recommends following the example of other jurisdictions and introducing a Duty of Care into the Act. Please see discussion and recommendations above at paragraphs 4.5.1 – 4.7.3.

2) Electronic service provider reporting

9.2.1. Section 474.25 of the Criminal Code Act 1995 sets out an obligation for service providers to notify the AFP of suspected child abuse material "within a reasonable time" of becoming aware of the material; however, there is little guidance as to what information should be provided to the AFP.

9.2.2. Other jurisdictions have more specific requirements for reporting to law enforcement. Part 4, Chapter 2 of the UK's Online Safety Act of 2023[56] requires platforms not reporting to NCMEC (the US-based National Center for Missing & Exploited Children) to report to the UK's National Crime Agency suspected child sexual exploitation and abuse on their platforms. The UK Act also empowers the Secretary of State to establish specific regulations regarding information in the reports,[57] format of the reports, the timeframe for sending those reports, and record keeping requirements.

9.2.3. In the US, the REPORT Act of 2023 establishes more substantive penalties for failure to report content. Companies that knowingly and wilfully fail to make a report of suspected CSAM can be fined up to $850,000USD ($1,285,608 AUD) depending on monthly active users. In a second or subsequent failure to make a report, the fine can be raised to $1,000,000USD ($1,512,480 AUD) depending on monthly active users.

9.2.4. IJM recommends that in conjunction with Australia's OSA industry codes that require companies to proactively detect CSAM, the reporting requirements of electronic service providers should be strengthened. Similar to the UK's legislation, the OSA should establish provisions for tech companies to report to the Australian Federal Police (AFP) directly if they do not already report to NCMEC's CyberTipline, and establish powers for eSafety to determine what information will be required to be reported by appropriate services, the timeframe for sending those reports, and detailed record keeping and content preservation requirements.

Recommendation 13: Require digital services and platforms who are not making reports of suspected child sexual exploitation and child sexual exploitation material to

[56] https://www.legislation.gov.uk/ukpga/2023/50

[57] See also Stanford Cyber Policy Center's research on NCMEC's CyberTipline recommending that additional research for types of reported content to NCMEC be considered. The Strengths and Weaknesses of the Online Child Safety Ecosystem (2024) Stanford Cyber Policy Center https://cyber.fsi.stanford.edu/io/news/cybertipline-report#:~:text=A%20new%20Stanford%20Internet%20Observatory,online%20child%20abuse%20reporting%20system.

NCMEC to report suspected child sexual exploitation and child sexual exploitation material to the Australian Federal Police. Provide the Commissioner with powers to mandate the type of information to be included in the reports and the timeframe for sending those reports. Establish detailed record keeping/content preservation requirements and more appropriate penalties for failure to report content in line with requirements under industry codes and standards.

3) Survivor-centric review mechanisms

9.3.1. One of the primary online safety bills being considered in the United States is the EARN IT Act (S. 1207).[58] This bill was first introduced by the United States Senate, and has been unanimously passed by the Senate Judiciary Committee on three separate occasions, receiving bipartisan support. One of its key functions is to establish a commission of experts to develop best practices related to combatting online sexual exploitation and abuse online. Some of the experts on this panel would be survivors and can include survivors from other jurisdictions to appropriately and holistically consider the global nature of crimes against children online.

9.3.2. IJM recommends that the Online Safety Act establish specific provisions for survivor consultation when developing regulatory frameworks or amending criminal codes related to online child sexual exploitation and abuse.

9.3.3. Survivors have spoken out about the devastating impact of the abuse perpetuated against them with the following words:

> "A lot of young people have been abused and many of them commit suicide because of what happened to them. It's not just mental health, it affects the child's background. It also affected their family life. We don't want children to experience this – especially our future children. Its effects are grave and our recovery was not easy."[59]

9.3.4. See also the attached letter from the Global Survivor Network to hear direct feedback from survivors on the necessary amendments to the OSA in order to protect children across the globe from this type of horrific abuse.

Recommendation 14: Establish a mechanism within the Act for consulting individuals with lived experience such as survivors of child sexual exploitation or abuse online when developing or amending regulatory frameworks or criminal law provisions related to online child sexual exploitation and abuse.

4) Safety technology development

9.4.1. Section 121 of the UK's OSA[60] establishes a process by which digital service providers can be compelled to deploy accredited technology to identify and prevent CSEA content, whether that content is communicated publicly or privately. Additionally, it allows for providers to be compelled to use the provider's best endeavours to develop or source technology to accomplish those same purposes. By establishing specific provisions for the UK regulator, Ofcom, to develop the accreditation process and establish a list of technologies that can prevent CSA, the UK has allowed for innovative solutions to develop and mandate child protection to both protect children experiencing harm now and other ways in which online sexual exploitation of children might develop as a crime in the future.

[58] https://www.congress.gov/bill/118th-congress/senate-bill/1207

[59] https://www.ijmuk.org/stories/survivor-letter-to-uk-government-online-safety-bill

[60] https://www.legislation.gov.uk/ukpga/2023/50/section/121

Recommendation 15: Establish a process of accreditation for safety technologies that can prevent and address child sexual exploitation and child sexual exploitation material and have eSafety maintain a public register of accredited technologies.

5) Restitution

9.5.1. US legislation provides for a mandatory court order of restitution where a defendant is convicted of certain crimes, such as CSAM-related crimes. The proposed STOP CSAM Act in the US establishes an amendment to 18 USC 1593 to establish that the "Restitution amount is no less than $3,000 or 10% of the full amount of victim's losses, if the full amount of those losses is less than $3,000." This piece of US legislation aptly demonstrates that one critical component of combatting this horrific crime is ensuring restitution for survivors.

9.5.2. Australia currently does not have a national compensation scheme for victims of Commonwealth crimes, including victims of online child sexual exploitation. The alternative of pursuing restitution from the defendant through criminal law proceedings is legally complex and costly, and thus not accessible for many survivors.[61] We recommend that Australia provide an accessible pathway to compensation that is available to all victims of online sexual exploitation.

Recommendation 16: Bring in amendments to criminal law to provide a pathway for compensation to victims of online sexual exploitation that is easily accessible for domestic and foreign victims and covers medical services such as physical, psychiatric or psychological care, social services, transportation, legal expenses and other relevant losses incurred by the victim.

6) Register of risks and risk profiles

9.6.1. Section 98 of the UK's OSA establishes a register of risks and risk profiles regarding risk of harm to individuals, risk of harm to children, the identification of risks specific to platform functionality, and the requirement for Ofcom to provide guidance on risk mitigation for each service based on its determined risk profile. This type of transparency and public reporting establishes a clear framework for accountability that gets to the root of many online safety issues – platform functionality. Because platforms are not built safe by design and allow for the easy livestream of child sexual abuse, platforms with 1:1 or private livestream functionality are inherently risky and should be flagged accordingly. The Australian government should consider including the development of a functionality-based risk register to tackle the highest risk features and support accountability for building platforms safe by design.

Recommendation 17: Require digital service providers to undertake risk assessments that identify risk of harm to users generally, specific risk of harm to children and other vulnerable groups, and risks specific to platform functionality. Establish a publicly available register of risks and risk profiles.

[61] In the two instances where victims of Commonwealth child sexual abuse offences pursued reparations under s. 21B of the Crimes Act 1914 and received a settlement from the defendant, the victims were represented by legal counsel, who rendered many hours of legal services on a pro bono basis. See sentencing remarks in DPP (Cth) v. Cooper [2021] VCC 1515. See also reference to R v. Moyle [2022] SASCA 61 at https://www.abc.net.au/news/2022-06-22/adelaide-paedophile-geoffrey-william-moyle-sentence-extended/101173814

Q33: Should Australia consider introducing a cost recovery mechanism on online service providers for regulating online safety functions? If so, what could this look like?

10.1.1. The implementation of online safety functions should be a requirement for digital service providers, not an "extra"; the entities who are members of the digital sector should cover the costs for the administration of Australia's online safety regime. The Act should make provision for a cost recovery mechanism, in keeping with jurisdictions such as the UK, EU, Ireland and Canada (proposed), for the purpose of recovering all, or a portion of, the costs incurred to administer the Act, including costs incurred by the eSafety Commissioner in the performance of their duties and functions.

10.1.2. This could be an annual cost recovery levy payable by entities covered by the industry codes and standards, calculated by reference to the service provider's worldwide revenue – similar to the cost recovery under UK's OSA – or on the basis of a formula set out in a legislative instrument, in a manner similar to the calculation of the Australian Securities and Investments Commission's (ASIC) Supervisory cost levy.[62] The amount of the total levy payable by entities would be no greater than the amount of eSafety's regulatory costs for the financial year. Penalties should apply for failure to pay the annual levy.

Recommendation 18: Australia should introduce an annual cost recovery levy on online service providers that covers the costs for administering the Online Safety Act.

IV. About IJM

International Justice Mission (IJM) is a global organisation that protects people in poverty from violence. As the largest anti-slavery organisation in the world, IJM partners with local authorities in 31 program offices in 16 countries to combat slavery, violence against women and children, and other forms of abuse against people who are poor. IJM works with local authorities and governments to rescue and restore survivors, hold perpetrators accountable, and help strengthen public justice systems so they can better protect people from violence.

V. About IJM's Center to End Online Sexual Exploitation of Children

IJM's Center to End Online Sexual Exploitation of Children protects children in the Philippines and scales the fight against this crime globally. The Center leverages and shares effective practices and models from IJM's Philippines program to enhance justice system and private sector responses to online sexual exploitation, resulting in sustainable child protection and offender accountability.

Contact:

John Tanagho
Executive Director
IJM's Center to End Online Sexual Exploitation of Children
LinkedIn| ijm.org.ph/Centerijm.org.ph/Center

Grace Wong
Chief Advocacy Officer
IJM Australia
[redacted] IJM.org.au

[62] See ASIC Supervisory Cost Recovery Levy (Collection) Act 2017 and ASIC Supervision Cost Recovery Levy Act 2017.

Annex I:

Case Examples: Livestreamed Child Sexual Abuse and CSAM Production

Below are 29 examples of cases where offenders sexually abused and exploited children, including directing and consuming the abuse in real-time via live video stream. These cases are particularly graphic, showing the horrific nature of new CSAM production in live video calls where perpetrators are unfettered by any sort of detection or disruption. These perpetrators have abused children **as young as infants.**

Most livestreaming cases are never identified or prosecuted and others are likely unreported in the news. See this study report from UK's University of Nottingham Rights Lab, which documented 30 cases beginning in 2010 involving UK offenders using specific platforms to livestream child sexual abuse.[63]

Date	Abuse Description	Age of victim(s)
Livestreaming		
07/19/19 Man gets 30 years for making child porn using kids in PH | Inquirer	US-based offender directed Filipino facilitators to perform sexual acts on children (infants to age 10) while he watched via **Skype**, in exchange for money.	Infant to 10 years
04/08/2022 District of South Carolina | Beaufort County Man Sentenced to 30 years for Production of Child Pornography | United States Department of Justice	US-based offender admitted to assaulting a **22-month-old victim** approximately five times between September 2019 and December 2019, and live streaming these assaults over **Skype** to an offender in the UK.	22 months
05/16/2019 Convicted child sex offender behind bars again for illicit Skype relationship with Filipino children under the age of 12 (smh.com.au)	Over a 4-and-a-half-year period, Australia-based offender paid a Filipino family over $26,000 for continued livestreamed CSEM of two sisters (age 2 and 7 when the abuse began) via Skype.	2, 7
05/17/2017 'Dreadful' Devon child abuser jailed for 18 years - BBC News	UK-based offender paid Filipino facilitators and directed them via Skype as he watched and recorded 102 hours of livestreamed sexual abuse of up to 46 child victims.	2 through 15 years
10/19/21 Retired South Australian public servant Ian Schapel, 67, sexually exploited kids in the Philippines | Daily Mail Online	Australia-based offender directed adult Filipina women over Skype to perform sexual acts on children in exchange for money; he had at least 13 victims aged between three and nine years old who were abused on 74 occasions.	3, 9
07/29/29 Paedophile who paid Filipino mums for pictures of naked daughters is jailed | Metro News	Over a 3-year period, UK-based offender communicated with facilitators in the Philippines via Skype and provided 36 payments for CSEM of girls aged 5 to 12 years old.	5, 12
04/12/2019 Paedophile directed child abuse films on Skype 7,000 miles away from his home | Metro News	Over a 3-year period, UK-based offender paid 8 facilitators to carry out sex acts and livestream the abuse of female children (aged 6 and 9) in the Philippines via Skype.	6, 9
11/15/2021 British pensioner, 68, jailed for 12 years relating to sexual exploitation of child in Philippines | Daily Mail Online	UK-based offender admitted to 67 separate offences, including using Skype to contact the mother of the child in the Philippines and making online payments in order to facilitate the sexual exploitation of the child victim and sending images of the abuse.	6

[63] "Legal and institutional responses to the online sexual exploitation of children," University of Nottingham Rights Lab, September 2023, https://www.nottingham.ac.uk/research/beacons-of-excellence/rights-lab/resources/reports-and-briefings/2023/october/legal-and-institutional-responses-to-the-online-sexual-exploitation-of-children-the-united-kingdom-country-case-study.pdf, page 10.

11/05/2021 Southern District of Ohio | Shelby County man sentenced to 27 years in prison for sending money to Filipino mothers in exchange for child pornography | United States Department of Justice	Over a 3-month period, US-based offender directed Filipino facilitators over Skype to share sexual images and videos of their children in exchange for payments via MoneyGram.	7
08/08/19 Office of Public Affairs | Kansas Man Sentenced for Producing Child Pornography | United States Department of Justice	US-based offender travelled to the Philippines to film himself engaging in sex act with minor females as well as communicating via Skype with a child's mother and directing her to livestream CSEM depicting an 8-year-old female.	8
05/23/2022 Twisted paedo 'used Fornite & Call of Duty to prey on kids & force them to pose naked as cops find 2,000 abuse images' | The US Sun (the-sun.com)	Previously convicted Spain-based offender made 81 payments to at least 26 victims between the ages of eight and twelve using online gaming platforms, then convinced them to appear naked on Skype.	9
05/23/2019 Ex-British army officer jailed for online child sex abuse in PHL | GMA News Online (gmanetwork.com)	Over a 2-year period, UK-based offender made nearly 50 payments to direct and view livestreamed child sexual exploitation material (CSEM) of multiple Filipino children via Skype.	9
12/18/20 Businessman admits paying for online child abuse from Philippines (bbc.com)	Over a 2-year period, UK-based offender directed an adult facilitator for livestreamed abuse of Filipino children (as young as 10 years old) via Skype, in exchange for over £5,500.	10
10/06/21 Jail for Victorian man who exploited girls in the Philippines (theage.com.au)	Australia-based offender directed 13-year-old Filipina girl over Skype to undress and perform lewd acts in exchange for money. Other victims were aged 11 and 12.	11, 12
02/01/2022 Winnipeg man wanted in Philippines for allegedly paying to watch child sex abuse: search warrant | CBC News	Canada-based offender is wanted for wiring thousands of dollars to facilitators in the Philippines for child exploitation offenses including livestreaming the sexual abuse of children via Skype. This is also the case of "Daisy's Destruction" (**the video series of an 11-year-old girl being raped, tortured, and murdered**).	11
02/28/2022 Ex-DJ Mark Page 'arranged sex with Philippine children' (bbc.com)	UK-based offender is charged with multiple child exploitation offenses that occurred from 2016 – 2019, including directing Filipino children to perform sexual acts over Skype in exchange for money.	12
10/27/2019 Sydney man accused of 'live-streaming child abuse' is arrested - as girl is saved in the Philippines | Daily Mail Online	A 63-year-old man has been accused of live-streaming child abuse from his Sydney home - as a 12-year-old victim is rescued in the Philippines.	12
06/30/2018 Five years in jail and worldwide travel ban for British teacher who wanted to abuse young Filipino children - National Crime Agency	UK-based offender sent at least 15 wire transfers to adult facilitators in the Philippines for images and livestreamed videos of children being sexually exploited; in addition, he attempted to arrange travel to the Philippines over Skype conversations.	12, 13 (he describes wanting to exploit children ages 4, 6, 9).
3/2/2022 BBC Radio DJ Mark Page, 63, 'flew to the Philippines to have sex with girl, 13, sent graphic messages about what he wanted and asked a girl, 14, to carry out	A former radio executive allegedly flew to the Philippines to sexually abuse/exploit a 13-year-old girl and sent graphic messages about sex acts he wanted performed, a court has heard. Three of the offences were said to have occurred in 2016 on **webcams**, when he was in the UK and the children were in the Philippines, Teesside Crown Court was told. The remaining two offences were said to have happened in person after Page, who was also a DJ, travelled to the Philippines. Prosecutor Jo Kidd told the	12, 14

sex acts on a 12-year-old', court hears	jury he set up a Facebook profile in the name of 'Thai G' and used it to contact a 13-year-old girl whilst in the Philippines in March 2019, before promising her 1,000 pesos. The court heard that Page sent graphic messages about sex acts he wanted the school children to perform. Page is alleged to have used his **Skype** account from his former Ingleby Barwick home to carry out explicit video calls with children online. He is alleged to have asked a 14-year-old girl to carry out sex acts on a 12-year old, but the prosecution say the older girl refused. In another chat, Page is accused of sending 1,500 Pesos to a girl after she allegedly performed sex acts over a **webcam** before messaging: 'I hope to visit you late October babe, and will you bring her to babe?'	
02/06/2022 Brooklyn Porn Arrest: Instagram, Skype Used to Target Kids, Feds Say – NBC New York	Over a 4-year period, US-based offender engaged in sexually explicit Skype communications with at least eight underage victims, in the U.S. and abroad, between the ages of 13 and 17. He was charged with producing child pornography after prosecutors alleged, he directed children to send him sexually explicit images and videos after targeting them via Skype.	13 through 17
03/12/2021 Kieran Creaven: Former RTÉ producer jailed for child sex abuse (bbc.com)	Among multiple child exploitation offenses, Ireland-based offender paid an adult facilitator in the Philippines to send him CSEM depicting a 13-year-old girl over Skype.	13
07/08/2022 Man who paid £18 per session for children to be sexually abused online pictured for first time - MyLondon	A security controller who arranged the sexual abuse of children in the Philippines and paid to watch it via live-stream has been jailed for three years.	13 through 16
11/10/2021 Man paid $40 to watch Filipino child abuse | The West Australian	On multiple occasions, Australia-based offender used Skype to direct livestreamed shows of girls under 16 in the Philippines in exchange for money. The 57-year-old Victorian man was later told that the girl, aged between 13 and 15, had to be taken to hospital after the first recording. This didn't stop Rivo.	13, 15
08/08/2022 The fall of a serial sextortionist | U.S. | EL PAÍS English (elpais.com)	Mexican-based offender was sentenced to 34 years in prison for the production of child pornography after using multiple social media platforms, including Skype, in a sextortion scheme that victimized more than 100 girls and women around the world.	15
02/21/2019 Eastern District of New York | Queens Man Sentenced to 15 Years' Imprisonment for Producing Child Pornography | United States Department of Justice	In two months, US-based offender paid and directed Filipino facilitators to engage in sexual acts with children and recorded over 50 video conferences depicting the abuse, some livestreamed via Skype.	Children, NA
12/14/2023 Office of Public Affairs | Man Sentenced to 25 Years in Prison for Paying Philippine Sex Trafficker to Live-Stream Child Sex Abuse | United States Department of Justice	A Maine man was sentenced to 25 years in prison for the production and distribution of child sexual abuse material (CSAM) depicting a minor in the Philippines. In addition, Zoll frequently recorded the live-streaming video calls, which he would then show to other individuals when instructing them to sexually abuse children during their own calls.	Children, NA
07/25/2019 Man jailed for streaming child sex abuse from Philippines (bbc.com)	A sales advisor who was the first person in Scotland to be convicted of live streaming abuse of children has been jailed for nine years. "Bell has instructed said abuse to take place by verbal and written communication to persons in the Philippines via internet message services."	Children, NA
01/25/2024 Sydney Man Faces Charges for Remote Child Abuse Orders | Mirage News	A Sydney man has appeared in the Downing Centre Local Court today (25 January, 2024) after being charged with allegedly paying to watch online as a child overseas was sexually abused.	Children, NA
10/14/2022 Man appears in court charged with sending money to Philippines to live stream child	The 71-year-old only spoke to confirm his not guilty pleas to the charges, 15 of arranging/facilitating the commission of a child sex offence and two of making indecent photographs of a child. Prosecuting, Ms Tolman told the court that on October 1 2020 the National Crime Agency (NCA) received	Children, NA

sexual abuse - Manchester Evening News	information that Grace had made an "illicit money transfer" to the Philippines.	
Production of CSAM in Images and Videos Cases Where Livestreaming May Have Occurred but Press or Prosecution Didn't Include It		
2/25/2022 South Florida Man Sentenced to 25 Years in Federal Prison for Exploiting Poor Children in the Philippines	Miami, Florida: Dennis Pollard used a social media messenger application* in 2020 to find young girls in the Philippines whom he could groom for the purpose of producing child sexual abuse material (CSAM). Pollard offered, and sometimes provided, money through wire services in exchange for pornographic images of the girls. Over nearly six-weeks, Pollard convinced a 13-year-old girl, living in poverty, to record herself performing sexual acts in exchange for money. Pollard also directed a woman in the Philippines to record herself sexually abusing her two toddler-aged children. Pollard distributed CSAM of his victims to groom others and obtain more CSAM. In 2015, Pollard attempted to produce CSAM through a different account on the same social media messenger application.	Toddler-aged, minors
04/20/2022 Zane Clark: Paedophile pleads guilty to child abuse, grooming charges | news.com.au — Australia's leading news site	Australian-based offender pleaded guilty to procuring a child under 16 for unlawful sexual activity and possessing and transmitting child abuse material, after using Skype to groom and approach the victim.	5
7/14/2022 UPDATE: Mother who pimped out 9 year old daughter jailed alongside 2 pedophiles	A mother was arrested yesterday for forcing her 9-year-old daughter into prostitution. The 26 year old woman, Chantra, was arrested after she posted sexy pictures of herself on Facebook, adding she had a child sex video and underage sex photos for sale. The post soon went viral on social media resulting in members of the public contacting police. Chantra confessed a man contacted her via Facebook in April last year asking to have sex with her daughter in exchange for 3,000 baht. The woman says she took the money because her family was poor. The young mother drove to a hotel in Nakhon Pathom province to meet the man and recorded him having sex with her daughter. She confessed she sold it to other men via Facebook for 500 to 800 baht at a time.	9
9/23/2022 Head teacher who groomed dozens of children on social media jailed	A British head teacher who groomed at least 131 children worldwide using social media has been jailed, the National Crime Agency (NCA) has said. Nicholas Clayton, 38 and from Wirral, used Facebook Messenger to contact children as young as 10, the NCA said. Children's charity the NSPCC voiced concerns that Meta, which owns Facebook, plans to introduce end-to-end encryption on its messaging platform. Andy Burrows, head of child safety online policy at the charity, said: "Clayton's case highlights the ease with which offenders can contact large numbers of children on social media with the intention of grooming and sexually abusing them." **Private messaging is the frontline of child sexual abuse online**. It's therefore concerning that Meta plans to press on with end-to-end encryption on Facebook Messenger, which will blindfold themselves and law enforcement from identifying criminals like Clayton."	10 (131 children total)
10/06/2023 Norfolk man jailed for child sex offences in the Philippines	A man 'stage managed' the sexual abuse of children in the Philippines by paying for videos of them, having described in "graphic and disgusting" detail what he wanted to happen to them. Hockley, of Canterbury Way, Thetford, appeared at court for sentencing having been previously found guilty of arranging or facilitating child prostitution or pornography in that *he intentionally arranged the sexual exploitation of children between May 1, 2015, and January 22, 2017*. He was also found guilty of three counts of making indecent photographs of children on or before August 17, 2017, two counts of distributing indecent photos of a child and one offence of possessing an extreme pornographic image. Charles Myatt, prosecuting, said those offences were discovered after police had taken devices belonging to Hockley in relation to another offence - sexual communication with a child under 16 between April 2 2017 and May 8 2017 - which he was also convicted of. Hockley had been communicating with the girl, then aged under 12, on **Facebook** in a sexual way "totally inappropriate for a girl of that age".	11

7/18/2022 Thai tutor arrested for making child porn with boys	An alleged pedophile wanted by the US and Thai Cyber police has finally been tracked down and arrested thanks to a local boxing gym owner. If found guilty the 20 year old part time teacher faces between three and 10 years imprisonment and a fine between 60,000 baht and 100,000 baht. The tutor, named Mai, sexually assaulted children between the ages of 7 and 15 years old, tricking them into making child pornography videos and making money by allegedly uploading them to the OnlyFans platform. A 31 year old woman named Somjit notified police that Mai promoted an OnlyFans account on Facebook, adding she was afraid he might sell child sex videos via that platform.	11 (17 total children)
6/29/2022 Former Montgomery County Teacher Pleads Guilty to Multiple Child Exploitation Offenses After Traveling to the Philippines to Have Sex with Children	PHILADELPHIA: United States Attorney Jacqueline C. Romero announced that Craig Alex Levin, 66, of King of Prussia, PA, pleaded guilty to six counts of child exploitation offenses before United States District Court Judge Harvey Bartle, III, stemming from his travel to the Philippines over a nearly three-year period for the purpose of engaging in illicit sexual conduct with minor children, some as young as 12 years of age. He also engaged in commercial sex trafficking by brokering the sale of a minor girl, who was pregnant at the time, for sex with an adult sex offender in exchange for money. Prior to and during his travels, Levin created and maintained Facebook accounts that he used to communicate with minors in the Philippines for the purpose of enticing them to engage in illicit sexual conduct with him during his visits to the island nation. In addition, the defendant used Facebook Messenger to send child pornography to minors in the Philippines.	11
9/14/2022 St. Paul man sentenced to 43 years for largest sextortion case in FBI history	ST PAUL, Minnesota: According to the U.S. Department of Justice, from 2015 through 2020 Vang "adopted the personae of real minor girls" and posed as real people to get other young victims to produce and send him child pornography. When they refused, Vang threatened to and did release their sexually explicit images and videos. The FBI identified 1,100 minors targeted by Vang. There are victims in every state – including 50 in Minnesota – and in 13 other countries. The victims range from 12-17 years old. Born said Vang used dozens of usernames and IDs across different communications or social media platforms such as Skype, Snapchat, Facebook and Kik to lure minors into thinking that they were talking to another minor.	12-17 (1,100 minors targeted)
2/5/2022 Teen girls duped into sending nude photos	Two men have been arrested in two locations for allegedly duping girls aged 13-15 to send them nude photos and videos of themselves in exchange for online game items. The arrests were made following complaints that some Facebook users had approached girls aged 13-15 to send their nude photos and videos in exchange for items that could be used in online games.	13, 15
5/23/2022 Former Federal Agent Found Guilty of Enticing a Minor and Engaging in Sex Tourism in the Philippines	East St. Louis, Illinois: A Cahokia, Illinois, man was found guilty as charged last week for Enticement of a Minor, Travel with Intent to Engage in Illicit Sexual Conduct, and Engaging in Illicit Sexual Conduct in a Foreign Place. According to evidence presented during trial, Joseph Albert Fuchs, III, an American citizen, met a 14-year-old girl while visiting the Philippines. Fuchs then engaged in sexual conversations with the minor using Facebook. During those conversations, Fuchs discussed ways to evade detection of her age when he would return to the Philippines to engage in sexual acts with her at a hotel. Fuchs then returned to the Philippines in March of 2019 and engaged in sexual acts with the 14- year-old minor.	14
4/28/2022 Vallejo Man Pleads Guilty to Flying to the Philippines with the Intention of Engaging in Sexual Conduct with a Child	SACRAMENTO, California: Balbino Sablad, 80, of Vallejo, pleaded guilty today to traveling with the intent to engage in illicit sexual conduct, U.S. Attorney Phillip A. Talbert announced. According to court documents, in 2019, Sablad flew to the Philippines with the intention of engaging in sexual conduct with a child under the age of 16. Using Facebook, Sablad had engaged in sexual chats with a person he believed was the intended minor victim and he sent the intended minor victim over $2,000 prior to his travel to the Philippines. Before he arrived, he also discussed with a co-conspirator his plan to sexually abuse the intended minor victim in the Philippines.	Under the age of 16
3/23/2022 Schemer using Facebook for sex with minors arrested in Iligan City	ILIGAN CITY, Philippines: A scheming netizen using Facebook to lure women into illicit sex was entrapped here Tuesday by agents of the National Bureau of Investigation. Dimaporo told reporters Austria would first offer women money in exchange for footages of them naked via online	NA

	Messenger and threaten to circulate the obscene video clips if they refuse to have sex with him.	
6/8/2021 Oil City Man Pleads Guilty to Child Sexual Exploitation Charge; Judge Detains Him Pending Sentencing	Brent Lockwood, 63, pleaded guilty to one count before United States District Judge Stephanie L. Haines. In connection with the guilty plea, the Court was advised that Lockwood received computer images depicting minors engaging in sexually explicit conduct. The Court was also advised that Lockwood repeatedly expressed, during Facebook chats, his desire to travel to the Philippines for the purpose of engaging in illicit sexual activity with minor females.	Minors, NA
5/25/2022 Exploiting Philippine minors through Facebook lands Texan in federal prison	BROWNSVILLE, Texas: A 47-year-old Harlingen man has been ordered to federal prison following his conviction of receiving child pornography, announced U.S. Attorney Jennifer B. Lowery. At the time of his plea, Machietto admitted that from Dec. 1, 2017, to June 1, 2018, he used Facebook to communicate with minor girls located in the Philippines. He requested nude photos of them and sent money as compensation to their families.	Minors, NA
2/17/2022 Granite Falls man accused of possessing child pornography	Granite Falls, MN: James Leroy Sanborn, 85, of Granite Falls, MN is facing four felony charges for being a predatory offender allegedly possessing pornographic photos and videos involving minors. The images in his possession were allegedly sent to him by families in the Philippines that he was helping to support. According to the criminal complaint, Sanborn said during an interview that he might have images and videos on his phone and on his Facebook Messenger app. He said he sent money to five or six families in the Philippines. He said the money was to help them recover from fires and floods or send their children to school.	Minors, NA
10/14/2022 District of Minnesota | St. Paul Man Sentenced to 43 Years in Prison for Targeting More Than 1,100 Minor Victims in Sextortion Scheme | United States Department of Justice	Over a period of several years, US-based offender victimized more than 1,000 young girls through a sextortion scheme that utilized multiple social media platforms, including Skype.	Minors, NA (750 identified female minor victims)
10/14/2022 Aydin Coban sentenced to 13 years for sexual extortion of Amanda Todd | CBC News	Netherlands-based offender was sentenced to 13 years for extortion, two counts of possession of child pornography, child luring and criminal harassment after using multiple social media platforms, including Skype, to demand web shows from a teenage girl over a period of 3 years until she died by suicide.	Minor, NA
08/19/2022 District of Nevada | Las Vegas Man Sentenced To 12 Years In Prison For Distribution Of Child Sexual Abuse Material | United States Department of Justice	US-based offender was sentenced to 12 years in prison for distributing images of CSAM after Skype reported his account to the National Center for Missing and Exploited Children regarding the upload of files containing CSAM.	Minors, NA
12/22/2023 Utahn accused of 'sex tourism' faces numerous charges of child sex abuse | KSL.com	A Utah man suspected of engaging in "sex tourism" was arrested shortly after returning from the Philippines and police reported finding numerous files of child sex abuse material on his phone. Prosecutors have requested that Hunter remain in custody without the possibility of posting bail pending trial, noting that he "has been engaged in sexual behavior directed towards children for several decades. (He) has, by his own admission, paid for and directed the sexual abuse of children in other countries for his own sexual pleasure. (He) has travelled overseas for the express purpose of sexually abusing children," according to the charges.	Children, NA
7/16/2023 American gets 30 years in PH child porn case	A Chicago man has been sentenced to 30 years in prison for soliciting sexually explicit photos and videos from young girls in the Philippines. Karl Quilter, 58, pleaded guilty last year to sexual exploitation of children, the US Attorney's Office for the North District of Illinois said. Quilter enticed at least nine girls in the Philippines to produce sexually explicit photos and videos and send them to him via **Facebook, Viber and Skype** between 2017 and 2020, it said.	NA (9 girls in the Philippines)
8/1/2022 Man, 19, accused of offering and selling sex videos, nabbed in Cebu City	CEBU CITY, Philippines: A 19-year-old man, who was arrested for allegedly promoting and selling of self-produced videos of himself performing sexual acts to various male victims, including minors, underwent an inquest proceeding today, August 1, 2022. The National Bureau of Investigation	NA

	Central Visayas Regional Office (NBI CEVRO) in a statement identified the accused as Romilo Romero, 19, a resident of Barangay Bulacao in Cebu City. On July 29, 2022, a composite team of the National Bureau of Investigation Anti-Human Trafficking Division (NBI AHTRAD), NBI CEVRO, Department of Justice Inter-agency Council Against Trafficking (DOJ IACAT) from Manila, DOJ IACAT-7, and the Department of Social Welfare and Development (DSWD) conducted these two pronged operations: an entrapment and rescue operation and to serve a warrant to search, seize, and examine computer data. Allegedly, Romero used social media platforms such as **Facebook and Twitter to promote and sell sex videos**.	
7/29/2022 PNP seeks court aid to track down sexual predators on social media	MANILA, Philippines: The Philippine National Police (PNP) has sought a regional trial court's permission to acquire information from social media giants Facebook and YouTube about the people behind "Usapang Diskarte" – an online account encouraging child sexual abuse.	NA
7/12/2022 Convicted Sex Offender Sentenced to 20 Years in Prison for Child Pornography Offenses	A Greenfield man was sentenced today in federal court in Springfield for receiving child pornography. The defendant used Facebook messenger to communicate with a minor in the Philippines and receive pornographic images of the child. Fox induced a minor in the Philippines to engage in sexually explicit conduct for the purpose of producing images of that conduct. Specifically, Fox used Facebook messenger to communicate with the minor and to receive the pornographic images. In exchange for the images, Fox sent Western Union payments to the Philippines.	NA

Annex II:

"The Child Sexual Abuse Material Prevention Bill" or "CSAM Non-Compatible Bill" (sample language)

This proposed policy brief with sample bill language proposes that governments require, encourage, and/or incentivise device manufacturers to build their devices and manage their operating systems safe by design by embedding technology designed to prevent child sexual abuse material, including production, distribution, etc. Each section includes a rationale followed by sample language that can be adapted to fit into various jurisdiction legislative and/or regulatory legal frameworks and definitions.

Creating device level safety does not negate any electronic service provider ("ESP") or other social media or tech platform, app, or website online safety responsibilities. Instead, it creates an additional layer of harm mitigation and prevention at the device and operating system levels. Good examples of device or product level harm mitigation and safety tools in the offline world include seatbelts, air bags, brake assist, and anti-lock brakes embedded in automobiles. More recently, the U.S. Department of Transportation is preparing to require alcohol-impaired-driving prevention technology to be installed in all new passenger vehicles in order to prevent drunk driving accidents.[64]

Policy Objective #1: Child Sexual Abuse Material, including production, distribution, and possession, is illegal under numerous domestic laws and harmful to both victims and users. This policy objective is to require that devices come installed with CSAM prevention technology and be made incompatible with CSAM to eliminate or reduce the misuse of such devices. To meet this objective, the policy proposes to require devices that have cameras and that can connect to the internet to be installed with technology specifically designed to prevent the device from being misused to produce, share, or possess Child Sexual Abuse Material. The policy is for such devices to be built safe by design, making them safer for all users, including those under 18 years-old and adults.

Section i). seeks to define devices in scope by device type, entities in scope by entity role, and defines CSAM prevention and non-compatible with CSAM. The purpose of this section is to require the businesses to embed technology onto devices and Operating Systems to prevent CSAM.

i) All camera-enabled devices capable of connecting to the internet either through the device itself or by connecting to another device, including but not limited to mobile phones, tablets, laptops, game consoles, desktop computers and others (hereinafter "Device" or "Devices"), that are manufactured, sold, imported, exported, or operated in Australia shall have installed on them CSAM Prevention technology specifically designed to make the Device and its Operating System non-compatible with Child Sexual Abuse Material as defined below (hereinafter "CSAM") by blocking the production, rendering, displaying, distribution, transmission, upload, and storage of CSAM, inclusive of images and video (recorded and live video), including CSAM generated through artificial intelligence (hereinafter defined as "CSAM Non-Compatible Technology").

Policy Objective #2: Section ii) seeks to define CSAM for purposes of this bill to include two forms: first, all known CSAM (i.e. previously identified and categorized) because that CSAM is the easiest for technology to identify with the highest accuracy using hash-matching. There is no legal or valid reason to allow a Device as defined above and with the exceptions below to be capable of rendering, displaying, distributing, transmitting, uploading or storing known CSAM, because the material is illegal. Secondly, CSAM is defined to also include not-previously known or categorized/hashed CSAM of pre-pubescent minors. The policy behind limiting the blocking of this new CSAM to pre-pubescent minors is to avoid "edge" cases of content involving individuals who are adults but appear younger, since image and video classifiers are predicting that the content is CSAM and less accurate than technology identifying known images; and to acknowledge that societal discussions are ongoing about the sharing by teens of intimate images. However, there is clearly no legal or valid reason to

[64] https://www.nhtsa.gov/press-releases/drive-sober-campaign-launch-winter-2023

allow a Device to be capable of rendering, displaying, distributing, transmitting, uploading or storing CSAM of pre-pubescent minors.

Companies can program a classifier to focus on prepubescent minors without verifying or estimating the age of the individuals in the content.

Sample language:

ii) For purposes of this Bill, CSAM is defined as a) known child sexual abuse material previously identified and included in an official hash list, and b) child sexual abuse material of pre-pubescent minors that has not previously been categorized or hashed.

Policy Objective 3 seeks to mitigate expected attempts by offenders to bypass CSAM non-compatible technology.

Sample language:

iii) CSAM Non-Compatible Technology shall be installed on all Devices in such a manner as to minimize to the extent practicable the ability of users to circumvent the effective operation of such technology, for example by embedding it in the Operating System or other device hardware.

Policy Objective 4 seeks to limit privacy impacts on users of the implementation of CSAM non-compatible technology by not requiring companies to receive indication of, have access to, process, or store any CSAM blocked by the technology. In essence, the technology embedded on the Device does the work of blocking and preventing the harm, but no company is required to become aware of the content. Depending on the jurisdiction, lack of awareness of the attempted CSAM production, distribution etc. may limit company reporting obligations. A lack of reporting may serve to make this bill more palatable by reducing the impact of any technological error because it does not lead to a report.

Sample language:

iv) No entity or individual responsible for the manufacture, sale, import, or export of a Device or for the manufacture, management, or implementation of any Operating System or hardware installed with CSAM Non-Compatible Technology shall be required to receive indication of, have access to, process or store CSAM blocked via the technology.

Policy Objective 5 seeks to address jurisdictional legal concerns that may prohibit the government from requiring private entities to conduct searches that would violate Constitutional or other civil rights.

Sample language:

v) The functioning of CSAM Non-Compatible Technology does not require any entity or person to conduct any search, seize any content, or file reports in connection with instances of the blocking of CSAM.

Policy objective 6 is to ensure that technology used meets certain requirements and criteria to engender trust and reduce misuse or ineffectiveness of the technology, in order to balance the need for blocking CSAM with human and civil rights.

Sample language:

vi) CSAM Non-Compatible Technology shall be accredited by an approved body, such as a national regulatory body, or for governments without a regulatory body, accredited by a member of the Global Online Safety Regulators Network, taking into consideration accuracy, efficacy, security, auditability, cost, and privacy. An external human rights and applicable civil rights impact assessment shall be conducted as part of the accreditation process.

Policy Objective 7 is to exempt devices that are used for official and legal purposes in order to reduce the burden on businesses operating in technical and/or niche markets from unnecessary CSAM non-compatibility technology requirements and to prevent any impact on the lawful processing of CSAM by justice officials and qualified entities.

Sample Language:

vii) The following devices shall be exempt from compliance with this Bill: devices designed and used exclusively as security or surveillance cameras; by law enforcement investigating child sexual exploitation; by authorized non-law enforcement child protection entities such as Internet Watch Foundation, NCMEC, Canadian Centre for Child Protection; medical devices and equipment for use by medical professionals, for public safety and police cameras, devices used in approved scientific or medical labs for research, used by military or intelligence agencies, devices installed to assist in the operation or security of transportation vehicles, such as forward, rear, and side facing cameras, and self-driving cameras used in automobiles, boats, planes, trains and buses.

Policy Objective 8: Provide penalties for businesses within scope of the bill who violate its requirements.

viii) Penalty provisions for manufacturers.

Policy Objective 9: Provide penalties for users who misuse exempt devices to commit crimes related to child sexual abuse material.

ix) Penalty provisions for users of exempt device, potentially sentencing enhancements or aggravating factors.

Policy Objective 10: Provide a sunset provision allowing for sufficient time for businesses in scope to comply with the law through technology development, procurement, integration and implementation.

Sample Language:

x) The requirements of this Act shall become effective no later than 24 months after being enacted or signed into law.

*Or other term in domestic law that is equivalent to CSAM.