Justice & International Mission
Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA

Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600
E-mail: le.committee@aph.gov.au

Supplementary Submission by the Synod of Victoria and Tasmania, Uniting Church in Australia to the inquiry into law enforcement capabilities in relation to child exploitation
14 October 2022

The Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes this opportunity to make a supplementary submission to the inquiry into law enforcement capabilities in relation to child exploitation.

The Synod is deeply concerned about serious human rights abuses that occur online or are facilitated online, including child exploitation. The Christian faith, as understood by the Uniting Church in Australia, teaches that all people are made in the image of God and all are valuable. There is a need to protect the most vulnerable from abuse and exploitation.

We continue to believe there is a need for additional legislative tools to combat online child exploitation. In June 2022, the US Federal Trade Commission in its report to Congress stated:[1]

> *Legislative efforts around the world may reflect that the only effective way to deal with online harms are laws that change the business models or incentives allowing harmful content to proliferate.*

The fight against child sexual abuse is my number one priority. And the most powerful weapon I have in this fight is legislation.[2]

Ylva Johansson – European Commissioner for Home Affairs

It hurts me to know someone is looking at them – at me – when I was just a little girl being abused for the camera. I did not choose to be there, but now I am there forever in pictures that people are using to do sick things. I want it all erased.

Testimony of a survivor[3]

[1] US Federal Trade Commission, 'Combatting Online Harms Through Innovation. Federal Trade Commission, Report to Congress', 16 June 2022, 74.
[2] Chloe Setter, 'Online safety laws can help to turn the tide against child sexual abuse online', We Protect Global Alliance, 4 May 2022.
[3] US National Centre for Missing and Exploited Children, 'End-to-End Encryption: Ignoring Abuse Won't Stop It', https://www.missingkids.org/e2ee

The Synod welcomes that since it made its submission to the Committee the Parliament has passed the *Telecommunications Legislation Amendment (International Production Orders) Act 2021.*

Some of the multinational technology corporations have also implemented modest reforms on their platforms in response to increasing legislative action by governments. For example, in response to the UK Age Appropriate Design Code:[4]

- Instagram no longer allows unknown adults to direct message under 18s (although the measure will only be effective against predators if it can screen to detect when an adult is falsely trying to open an account as a child);
- TikTok users under the age of 16 will have the accounts set to private by default;
- Google will stop targeting advertising to identified users under the age of 18; and
- YouTube committed to removing autoplay, to prevent children being fed endless videos.

Corporations that breach the Age Appropriate Design Code and put children at risk can be fined up to £17.5 million or 4% of their annual worldwide turnover.[5] The Code requires corporations to ensure their digital products and services must be designed in the best interests of children. The Code specifically states that the best interest of a child must be accounted as a primary consideration when in conflict with commercial interests.[6]

The EU has been moving on a proposal that would require corporations offering services in the EU to detect, report and remove child sexual abuse material online irrespective of their place of establishment. The corporations would be required to use the least intrusive measures to achieve the objective. The technology used would not be able to extract any other information than what is strictly necessary to detect the abuse. Detection orders will be issued by courts or independent national authorities.[7]

Whatsapp has stated that it detects and bans two million accounts every month based on abuse patterns and scans unencrypted information, such as profile and group information for abusive content, like child exploitative imagery.[8] However, Whatsapp did not reveal whether it shares any intelligence from its actions with law enforcement agencies.

There is evidence that the number of victims of online child sexual abuse is underestimated. For example, interviews with children across 12 countries in the East Asia and Pacific and Eastern and Southern Africa regions during 2020 to 2021 indicated that between one and 20% of children suffered online sexual exploitation and abuse in the past year. Only one in three told anyone about the abuse they suffered.[9] ECPAT, INTERPOL and UNICEF reported that in the past year, 20% of internet users aged 12 to 17 in the Philippines were victims of:[10]

> *… grave instances of online sexual exploitation and abuse. This includes being blackmailed to engage in sexual activities, someone sharing their sexual images*

[4] 5Rights Foundation, 'Raft of tech changes to protect children as new rules come into force', 2 September 2021.
[5] Ibid.
[6] Ibid.
[7] European Union, 'Fighting Child Sexual Abuse', #EUvsChildSexualAbuse, 11 May 2022.
[8] Will Cathcart and Stan Chudnovsky, Letter in reply to the Rt Hon Priti Patel MP, William P Barr, Chad F Wolf and the Hon Peter Dutton MP, 9 December 2019.
[9] UNICEF, 'Legislating for the digital age: Global guide on improving legislative frameworks to protect children from online sexual exploitation and abuse', May 2022, 5.
[10] ECPAT, INTERPOL and UNICEF, 'Disrupting Harm in the Philippines: Evidence on online child sexual exploitation and abuse', Global Partnership to End Violence Against Children, 2022, 11.

without permission, or being coerced to engage in sexual activities through promises of money or gifts.

ECPAT, INTERPOL and UNICEF reported that of those aged 12 to 17 that experienced online sexual abuse on social media, 90% occurred on Facebook or Facebook Messenger.[11]

Recommendations

In addition to the suggested recommendations put forward in our first submission, the Synod requests that the Committee make the following additional recommendations:

- That the current regime of ISPs being required to disrupt ready access to online child sexual material contained on the INTERPOL 'worst of' list[12] using Section 313 of the *Telecommunications Act 1997* be extended to cover a wider range of child sexual abuse material. For example, the INTERPOL list could be supplemented by the Internet Watch Foundation list. Further, data from attempts to access disrupted material could be provided to the Australian Federal Police in a format that would allow police to analyse and detect users that have a pattern of attempting to access such material. The recommendation has also been made by ECPAT, INTERPOL and UNICEF.[13]
- As suggested by UNICEF, laws could be introduced to require online technology corporations to have to detect proactively child sexual abuse material accessed or stored on their platforms or services for the purpose of blocking or removing such materials.[14] The detection of such material should also be reported to reported to the Australian Federal Police in a format specified that would allow the police to make effective use of the reports.[15] Such an obligation is consistent with obligations of reporting obligations of entities subject to the *Anti-Money Laundering Counter-Terrorism Financing Act 2006* and the increasing push towards human rights due diligence obligations. UNICEF has already drawn an analogy between the European Commission proposal for a Directive on corporate sustainability and due diligence with an obligations for technology corporations to implement forms of due diligence to detect and report online child exploitation.[16] ECPAT, INTERPOL and UNICEF have recommended that technology platforms provide law enforcement agencies with any associated information they have that might help to identify offenders and victims in a timely manner.[17]
- As per our previous submission, the online platforms must make their avenues to report online child sexual abuse clear, accessible and easy to use. The recommendation has also been made by ECPAT, INTERPOL and UNICEF.[18]

Use of encryption, encryption devices, anonymising technologies and Remote Access Trojans and resources of law enforcement to address their use

[11] Ibid.
[12] https://www.interpol.int/en/Crimes/Crimes-against-children/Blocking-and-categorizing-content
[13] ECPAT, INTERPOL and UNICEF, 'Disrupting Harm in the Philippines: Evidence on online child sexual exploitation and abuse', Global Partnership to End Violence Against Children, 2022, 110.
[14] UNICEF, 'Legislating for the digital age: Global guide on improving legislative frameworks to protect children from online sexual exploitation and abuse', May 2022, 26.
[15] Ibid., 26.
[16] Ibid., 89.
[17] ECPAT, INTERPOL and UNICEF, 'Disrupting Harm in the Philippines: Evidence on online child sexual exploitation and abuse', Global Partnership to End Violence Against Children, 2022, 110.
[18] ECPAT, INTERPOL and UNICEF, 'Disrupting Harm in the Philippines: Evidence on online child sexual exploitation and abuse', Global Partnership to End Violence Against Children, 2022, 110.

As a survivor of child sexual abuse imagery I still use social media every single day. As someone who has already entrusted the tech industry with so much I trust that you will work with child protection agencies to ensure that end-to-end encryption does not create a safe haven for paedophiles. I plead, as someone who has felt the pain and deals with the lifelong repercussions of this horrendous crime, that you not extinguish what little light we have on the horizon.[19]

Encryption is either something that is completely good or bad. Widespread adoption of encrypted web protocols like https have made a positive contribution. Standard encryption has improved how we can securely browse the web, access banking and government services, and communicate over e-mail and messaging apps. Until recently, privacy and security improvements have been largely compatible and complementary with the systems that have been protecting the safety of the most vulnerable users.[20]

Deploying end-to-end encryption in communication and social media platforms runs is direct opposition to protecting the safety of the most vulnerable users. It bypasses the tools technology companies are using to detect child sexual abuse content.[21] End-to-end encryption extends standard encryption, so that only the sender and receiver can view the content of messages. Thus, the platforms themselves are prevented from accessing any data being hosted on, or passed through, their systems. It is important to acknowledge that all popular messaging platforms are already using standard encryption, which protects our data from being incepted by third parties. The only real difference between end-to-end encryption and standard encryption is that the technology platform will no longer have any access to the content. Thus, it will not be able to use tools that can automatically detect images and videos of child sexual abuse that are being hosted or shared on their platforms.[22]

In the first half of 2021, due to an unintended consequence of new EU privacy laws, Meta stopped voluntarily scanning its platforms in the EU. During that time, the US National Centre for Missing and Exploited Children recorded a 58% reduction in reports of online child sexual abuse content. The reduction in detection demonstrates the disastrous consequence to curbing child sexual abuse online if automatic detection tools are blocked by end-to-end encryption.[23]

If automated detection tools cannot be made to work in end-to-end encrypted environments, millions of child sexual abuse images and videos will go undetected. Such an outcome would embolden offenders who will, correctly, understand their chance of getting caught has been reduced.[24] More children will be raped and abused as a result.

The US National Centre for Missing and Exploited Children (NCMEC) released an open letter on 20 February 2020 to the technology industry outlining five principles to safeguard

[19] US National Centre for Missing and Exploited Children, 'End-to-End Encryption: Ignoring Abuse Won't Stop It', https://www.missingkids.org/e2ee
[20] Dan Sexton, 'Not all Encryption is the same: social media is not ready for End-to-End Encryption', Internet Watch Foundation, 14 March 2022.
[21] Ibid.
[22] Dan Sexton, 'Not all Encryption is the same: social media is not ready for End-to-End Encryption', Internet Watch Foundation, 14 March 2022; and Julie Inman Grant and Jon Rouse, 'The rush to encrypt… and its unintended victims', Esafety Commissioner, 27 August 2019.
[23] Dan Sexton, 'Not all Encryption is the same: social media is not ready for End-to-End Encryption', Internet Watch Foundation, 14 March 2022.
[24] Ibid.

children in end-to-end encrypted environments:[25]

1. Do not implement end-to-end encrypted communications for accounts where a user has indicated they are under 18 years old;
2. Implement detection technologies, at least as effective or better than those currently available, to prevent offenders from distributing child sexual abuse material;
3. Adopt technology vetted by the child protection community to identify sexual grooming of children by adults;
4. Promptly report apparent child sexual exploitation to NCMEC's Cyber Tipline with actionable information to help rescue child victims and hold offenders accountable; and,
5. Ensure that law enforcement can use existing legal process to effectively investigate the sexual exploitation of children.

In October 2019, relevant ministers from the UK, US and Australia called on Facebook and other companies to take the following steps:[26]

- Embed the safety of the public in system designs, thereby enabling them to continue to act against illegal content effectively with no reduction to safety, and facilitating the prosecution of offenders and safeguarding of victims;
- Enable law enforcement to obtain lawful access to content in a readable and usable format;
- Engage in consultation with governments to facilitate this in a way that is substantive and genuinely influences their design decisions; and,
- Not implement the proposed changes until they can ensure that the systems they would apply to maintain the safety of their users are fully tested and operational.

The ministers stated that their technical experts had advised it was possible to protect users of the platforms and the public, while also protecting privacy. The response from Meta was to reject that view and argue, in effect, that privacy needed to override protecting children from sexual abuse on their platforms. Actions to address online child sexual abuse on their platforms would need to work separate from the implementation of end-to-end encryption.[27]

Dr Mark Zirnsak
Senior Social Justice Advocate

[25] US National Centre for Missing and Exploited Children, 'End-to-End Encryption: Ignoring Abuse Won't Stop It', https://www.missingkids.org/e2ee
[26] Rt Hon Priti Patel MP, William P Barr, Kevin K McAleenan and the Hon Peter Dutton MP, Letter to Mark Zuckerberg, 4 October 2019.
[27] Will Cathcart and Stan Chudnovsky, Letter in reply to the Rt Hon Priti Patel MP, William P Barr, Chad F Wolf and the Hon Peter Dutton MP, 9 December 2019.