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

Centre for Theology and Ministry
29 College Crescent
Parkville Victoria
Australia, 3052

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

# Response to Questions on Notice by the Synod of Victoria and Tasmania, Uniting Church in Australia to the inquiry into law enforcement capabilities in relation to child exploitation
# 2 December 2022

**Questions from Mr Sam Lim MP**

1. **Dr Mark Zirnsak, thank you for the submission on behalf of yourself and the synod. Online pornography is increasingly an accessible space that is the number one sexual educator of young people in Australia, and we can all agree that it should not be. But sites owned by MindGeek that largely make up the monopoly of online porn regularly feature child exploitation material and additionally pornographic material that is increasingly violent and unethical in nature. I wanted to know, do you believe that limiting initial access to such sites or requiring an age and ID verification to be able to access these sites would be of benefit to young people and limit the access and exposure of pornography that can lead to people eventually seeking gratification through CSEM?**

2. **Dr Zirnsak, I want to give you an opportunity to comment – is there anything that we have not asked you that you may want to include as part of these hearings? I would appreciate any further input you may have.**

As recommended in our submission to the inquiry, our strong preference is for the Committee to recommend the following:

- Technology providers must have robust systems to verify the identity of the people using their service. Identity verification would allow law enforcement agencies to increase the speed with which they can identify people suspected of being engaged in online child sexual abuse. It would also act as a general deterrent by reducing the perception that offenders will not be recognised for their online activities.
- Prohibit social media corporations from allowing children under 13 to open accounts on their platforms without verified parental or guardian consent.

While it is acceptable for the public-facing identity of a person to be anonymous, it is highly desirable for sites to have to verify the identity of people on platforms where they can interact with others. It would be easier to have systems where a person can have a digital identity that has been verified as their identity. That digital identity could be set up to identify when a person is under 18 to restrict their access to sites with inappropriate content for children.

The next best solution would be requiring robust age verification. While preventing a higher-determined teenager with sufficient technological knowledge from circumventing age verification may be impossible, it would shield many children from accessing inappropriate content.

In addition, as per our supplementary submission, we request the Committee recommend that the current regime of ISPs being required to disrupt ready access to online child sexual material contained on the INTERPOL 'worst of' list[1] using Section 313 of the *Telecommunications Act 1997* be extended to cover a broader 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. ECPAT, INTERPOL and UNICEF have also made the recommendation.[2]

Research presented by Sarah Napier at the 2022 Australian Institute of Criminology reported that they had surveyed 5,512 people between 2019 and 2021. Those surveyed reported:

- 93% of respondents had seen adult pornography while they were under 18 years of age;
- 70% had seen child sexual abuse material when they were under the age of 18;
- 64% had viewed S&M pornography when they were under the age of 18;
- 42% saw child sexual abuse material for the first time by accident when searching through adult pornography; and,
- 16.5% were sent unsolicited child sexual abuse material.

The research found that accidentally viewing child sexual abuse material led to 45% of respondents going on to then subsequently intentionally viewing child sexual abuse material.

The paper on these findings will be released in 2023.

Increasing the requirement for ISPs to disrupt access to known URLs hosting child sexual abuse material should help drive down the proportion of people, including children, that view the material for the first time while searching for adult pornography.

The February 2020 report by the House of Representatives Standing Committee on Social Policy and Legal Affairs '*Protecting the age of innocence. Report of the inquiry into age verification for online wagering and online pornography'* made the following assessment:

> *The Committee heard that as governments have sought to strengthen age restrictions on online content, the technology for online age verification has become more sophisticated, and there is now a range of age-verification services available which seek to balance effectiveness and ease of use with privacy, safety, and security.*
>
> *In considering these issues, the Committee was concerned to see that, in so much as possible, age restrictions that apply in the physical world are also applied in the online world.*
>
> *The Committee recognised that age verification is not a silver bullet and that protecting children and young people from online harms requires government, industry, and the community to work together across a range of fronts. However, the*

[1] https://www.interpol.int/en/Crimes/Crimes-against-children/Blocking-and-categorizing-content
[2] 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.

*Committee also concluded that age verification can create a significant barrier to prevent young people—and particularly young children—from exposure to harmful online content.*

*The Committee's recommendations, therefore, seek to support the implementation of online age verification in Australia.*

The Committee made the following relevant recommendations from that inquiry:

## *Recommendation 1*

*2.143 The Committee recommends that the Digital Transformation Agency, in consultation with the Australian Cyber Security Centre, develop standards for online age verification for age-restricted products and services.*

*a. These standards should specify minimum requirements for privacy, safety, security, data handling, usability, accessibility, and auditing of age-verification providers.*

*b. Consideration should be given to the existing technical standards in Australia and overseas, including but not limited to the UK Age Verification Certificate, the PAS 1296 Age Checking code of practice, the Trusted Digital Identity Framework, and the European Union General Data Protection Regulation.*

*c. Opportunities should also be provided for consultation with industry, including private age-verification providers and members of the public.*

## *Recommendation 2*

*2.148 The Committee recommends that the Digital Transformation Agency extend the Digital Identity program to include an age-verification exchange for the purpose of third-party online age verification.*

## *Recommendation 3*

*3.184 The Committee recommends that the Australian Government direct and adequately resource the eSafety Commissioner to expeditiously develop and publish a roadmap for the implementation of a regime of mandatory age verification for online pornographic material, setting out:*

*a. a suitable legislative and regulatory framework;*

*b. a program of consultation with community, industry, and government stakeholders;*

*c. activities for awareness raising and education for the public; and*

*d. recommendations for complementary measures to ensure that age verification is part of a broader, holistic approach to address risks and harms associated with the exposure of children and young people to online pornography.*

The Parliamentary Joint Committee on Law Enforcement should recommend that the above recommendations be implemented.

Concerning MindGeek, we note the current civil legal action in the US that has alleged that MindGeek was aware of and even encouraged the uploading of child sexual abuse material to its various websites. It is further alleged that the corporation monetised illegal material through advertising revenue.[3]

We note that the corporation has stated that it has strengthened its security measures by banning uploads from anyone who has not submitted a government-issued ID that passes third-party verification. In addition, it has further implemented technology that spots videos that violate its policies against non-consensual sexual material and child sexual abuse material.[4] While these measures are a step forward, it does not address the issue of children accessing inappropriate material on their platform. It therefore does not remove the need for the recommendations made above.

Dr Mark Zirnsak
Senior Social Justice Advocate

[3] National Centre on Sexual Exploitation, 'Judges Sides with Survivors of CSAM in Powerful Ruling Against Pornhub/MindGeek', 10 February 2022.
[4] Lateshia Beachum, 'Visa could be liable in suit over child sexual abuse material on Pornhub, other sites', *The Washington Post,* 1 August 2022.