The Uniting Church in Australia
QUEENSLAND SYNOD

Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA

Director – Strategy and Research
Online Safety, Media and Platforms Division
Department of Infrastructure, Transport,
Regional Development, Communications and the Arts
GPO Box 594
Canberra ACT 2601

E-mail: OSAReview@COMMUNICATIONS.gov.au

Joint submission by the Uniting Church in Australia, Synod of Queensland and the Synod of Victoria and Tasmania to the Statutory Review of the Online Safety Act 2021 Issues Paper

The Uniting Church in Australia, Synod of Queensland and Synod of Victoria and Tasmania welcome the opportunity to make a joint submission to the *Statutory Review of the Online Safety Act 2021* Issues Paper.

The Synods are deeply concerned about serious human rights abuses that occur online or are facilitated online, including child exploitation.

The Uniting Church in Australia has committed itself to support measures to address sexual abuse, including child sexual abuse. The 1991 National Assembly meeting of Uniting Church delegates from across Australia made the most explicit statement opposing all sexual abuse:

> *91.18.1/2 The Assembly resolved:*
> *To receive the report (of the Commission for Women and Men)*
> *(a) That sexual violence be deplored as a sin against God and humanity.*
> *(b) That it be recognised that the origin of sexual violence lies in the practice of inequality of the sexes;*
> *(c) That it be confessed that sexual violence is disturbingly frequent within the Uniting Church community as it is in the wider community;*
> *(d) That it be acknowledged that in the past, the church has often made inappropriate responses or no response to victims/survivors of sexual violence. This has been experienced by many as a further violation;*
> *(e) That the church be committed to hearing the voices of those who are victims of sexual violence;*
> *(f) That the actions of people who work for the end of such violence and who support its victims/survivors be supported;*
> *(g) That the urgent need for the church community to become part of a "network of prevention" in the area of sexual violence be recognised.*

Part 2 – Australia's regulatory approach to online services, systems and processes

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

The current objects of the Act are: to improve online safety for Australians; and to promote online safety for Australians. This is not sufficient, as the objects of the Act currently do not include improving online safety for people who are not Australians, but who experience harm as a result of Australians.

The objects of the Act should extend to address cyber-bullying of any child or any adult where the cyber-bullying has a connection to Australia. It should be an offence for anyone in Australia to engage in cyber-bullying of anyone, no matter their location or nationality. The Synods realise there will be many cases where it will be more difficult for law enforcement authorities to prosecute a cyber-bullying case involving a foreign national. Therefore, there will be cases that law enforcement agencies decide not to investigate or prosecute, as occurs with most crimes. However, the Bill should not signal that cyber-bullying is not a serious matter if targeted at foreign nationals.

In the Synods' view, the eSafety Commissioner should have a mandate to improve online safety globally where it is in Australia's interests to do so. Further, as noted above, the Commissioner should be authorised address online safety issues where harm is originating from Australia and its territories.

2. Does the Act capture and define the right sections of the online industry?

The Basic Online Safety Expectations within the Act establish minimum safety expectations for online service providers but cover a narrower spectrum of services than the Online Content scheme. The Basic Online Safety Expectations should apply to the same spectrum of services that the Online Content Scheme applies to.

3. Does the Act regulate things (such as tools or services) that do not need to be regulated, or fail to regulate things that should be regulated?

The Act does not regulate the unauthorised use of photographs and videos that are not 'indecent' but which are being used without permission from the person who's image is being used. We recommend that the federal government consider the best approach to regulating this issue, whether through the Act or through other legislation.

The Office of the Australian Information Commissioner (OAIC) provides guidance on dealing with photos or videos of a person taken without their permission and for photos or videos of a person posted online without permission**.** In Australia, if a photo or video was taken by someone acting in a personal capacity, the *Privacy Act 1988* doesn't apply as it doesn't cover individuals[1]. Photos and videos of a person are only treated as personal information under the *Privacy Act 1988* if the person's identity is clear or could reasonably be worked out, and an organisation takes the photo or video[2]. The *Privacy Act 1988* predominately covers organisations with an annual turnover of more than $3 million that operate in

[1] https://www.oaic.gov.au/privacy/your-privacy-rights/social-media-and-online-privacy/photos-and-videos
[2] Ibid.

Australia, with some other organisations included for certain purposes[3]. A number of factors go into deciding if an organisation operates in Australia, including if they have a presence in Australia or carry on a business in Australia[4].

The OAIC outlines the process for addressing this issue[5]: First, the person who's image is being used without their permission should ask the person who posted the photo or video online to take it down. If they refuse, or it is unable to be ascertained who it is, the site's administrator should be contacted and asked to remove the photo or video[6]. If they don't respond to the complaint, or if their response is unsatisfactory, a complaint can be lodged with the OAIC only if the photo or video posted online is hosted by an organisation or agency covered by the *Privacy Act 1988*[7].

A recent report by the Australian Institute of Criminology (AIC) details how predators use social media platforms or dating apps to track down people with access to young people, including parents or people who know children[8]. The AIC said "sharenting" – publishing information or photos of children online – "may place some children at risk of exploitation and harm"[9]. Respondents to the research who had publicly shared photos of or information regarding children online were especially likely to have received requests for facilitated child sexual exploitation (CSE), suggesting that educational initiatives and platform changes are required to minimise the risk of harm[10].

Of 4,011 Australians in the AIC survey, 2.8%, or 111 people, had received a request for facilitated CSE in the previous year[11]. Of those, 60 people had been asked questions of a sexual nature about children they knew; 38 were pressured for sexual images of children they knew; 40 were asked for such images; and 44 were offered payment for those images[12]. Among people who acknowledged posting a photo online of a child in their care or of another child they knew, the number was even higher, with 6.6% having received at least one request for facilitated CSE[13].

The AIC said parents or those who know children should think twice before posting photos in certain forums: "Given that it has become common practice for parents to share photos of their children online, concerted education efforts are needed to warn not just parents and guardians but all those who

---

[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] https://www.theguardian.com/media/2024/may/02/parents-share-photo-kids-online-identity-aic-report-sharenting Australian government warns against 'sharenting' as study finds 7% of people who post pictures receive request for child abuse material Josh Butler Thu 2 May 2024 12.18 AEST
[9] https://www.theguardian.com/media/2024/may/02/parents-share-photo-kids-online-identity-aic-report-sharenting Australian government warns against 'sharenting' as study finds 7% of people who post pictures receive request for child abuse material Josh Butler Thu 2 May 2024 12.18 AEST
[10] Prevalence and predictors of requests for facilitated child sexual exploitation on online platforms: Australian Institute of Criminology Trends & issues in crime and criminal justice No. 692 Savannah Minihan, Melanie Burton, Mariesa Nicholas, Kylie Trengove, Sarah Napier and Rick Brown
[11] Ibid.
[12] Ibid.
[13] https://www.theguardian.com/media/2024/may/02/parents-share-photo-kids-online-identity-aic-report-sharenting Australian government warns against 'sharenting' as study finds 7% of people who post pictures receive request for child abuse material Josh Butler Thu 2 May 2024 12.18 AEST

interact with children of the potential harms associated with publicly sharing photos of or information regarding children online" [14].

"If posting photos on private rather than public online platforms can reduce the risk of receiving requests for facilitated CSE, as the present findings suggest, this is a simple change that parents, guardians and others in a caregiving role could make," it said[15]. The federal Attorney General, Mark Dreyfus, also said "No parent would ever hand a photo album of their children to a stranger, and the same care should apply to photos posted online.".

The AIC noted that linguistically diverse individuals, people with disability and those who experienced other sexual or violent online harms also reported receiving higher rates of requests, stating that "particularly vulnerable" populations may require "targeted preventative efforts"[16].

Recently, short statured Australians reported that their photos are increasingly being taken without consent and posted on "m****t spotting" social media groups[17].There has been an influx of Facebook groups dedicated to soliciting photos of, and ridiculing short statured Australians with violent, derogatory and sexualised commentary[18]. The photos are being taken without their knowledge and consent and some photos show them going about their daily activities in public, while others were stolen from personal social media pages[19]. The short statured community wants authorities to be more proactive about abuse, and for the wider public to help call it out[20].

One of the people who has been photographed and placed on one of these pages said:
"[It] made me feel completely powerless, completely subhuman, and something that I don't want anyone else to have to experience…I'm actually feeling … unsafe because [the photos taken are] in my community,".

Despite being reported to Meta, the owner of Facebook, several groups were not removed[21]. According to communication seen by the ABC, the platform concluded at least one "did not go against our community standards"[22]. Complaints to the Office of the eSafety Commissioner were also unsuccessful - in one piece of correspondence seen by the ABC, the Commissioner's office agreed the content was "offensive and distasteful", but stated the situation was "outside of our legislative reason"[23]. A

[14] https://www.theguardian.com/media/2024/may/02/parents-share-photo-kids-online-identity-aic-report-sharenting Australian government warns against 'sharenting' as study finds 7% of people who post pictures receive request for child abuse material Josh Butler Thu 2 May 2024 12.18 AEST
[15] Ibid.
[16] Ibid.
[17] https://www.abc.net.au/news/2024-05-30/short-statured-community-call-out-online-abuse-facebook-groups/103896180 Short statured Australians are facing increased online abuse. They're asking for the public's help to stop it By the Specialist Reporting Team's Evan Young and Maryanne Taouk Posted Thu 30 May 2024 at 6:03am
[18] Ibid.
[19] Ibid.
[20] Ibid.
[21] Ibid.
[22] Ibid.
[23] Ibid.

spokesperson for the eSafety Commissioner said it could only flag content for removal when it met the threshold set out under the *Online Safety Act*, and also breached a platform's own terms of service[24].

One of the people who has been photographed and placed on one of these pages said she wanted the wider public to help in the fight against their abuse. "We need people who are not short statured to actually call this behaviour out when they see it"[25]. Short Statured People of Australia (SSPA) president Sam Millard said businesses also had a role to play in calling it out, given many of the photos and videos were recorded inside restaurants, shopping centres, and gyms[26]: "A lot of the time, people with a disability are the ones kind of policing the situation [and] that can become quite burdensome. If the wider community is, firstly, aware that this is happening in the first place and then be empowered to kind of step in and say, 'this is unacceptable', then I think that goes a long way".

The AIC also said the platforms themselves should be doing more to warn users about the potential dangers of posting too much information about children online[27]. Online platforms have a responsibility to mitigate harms and to warn users of the risks associated with particular online behaviours. For example, while Facebook, Instagram and TikTok prohibit the posting of material that sexually exploits or could lead to the sexual exploitation of children, there are no specific provisions regarding the posting of photos or information regarding children in general[28] . Similarly, dating apps such as Tinder and Bumble do not allow the posting of profile photos of unaccompanied or unclothed children, yet this does not prevent users from posting profile photos of themselves with children or sharing that they have children[29]. The AIC suggests that for example, online platforms could implement safety by design features, whereby a user receives a warning message upon attempting to upload a photo of or information regarding children to a public site[30].

The Canadian Centre for Child Protection (CCCP) has expressed deep concern that some hosting corporations will refuse to remove all images in a series that documents child sexual abuse[31]. Numerous images are often created in connection with an abusive series, some of which in isolation would not meet the legal definition of child sexual abuse material but are still part of the continuum of abuse experienced by the child[32]. For example, a series may start with an image of a child being clothed and then the images progress to the child being sexually abused[33]. The CCCP argues that the clothed image is still a memorialisation of the child's abuse and should be removed.[34] Such images are typically used to

---

[24] Ibid.
[25] Ibid.
[26] Ibid.
[27] https://www.theguardian.com/media/2024/may/02/parents-share-photo-kids-online-identity-aic-report-sharenting
Australian government warns against 'sharenting' as study finds 7% of people who post pictures receive request for child abuse material Josh Butler Thu 2 May 2024 12.18 AEST
[28] Prevalence and predictors of requests for facilitated child sexual exploitation on online platforms: Australian Institute of Criminology Trends & issues in crime and criminal justice No. 692 Savannah Minihan, Melanie Burton, Mariesa Nicholas, Kylie Trengove, Sarah Napier and Rick Brown
[29] Ibid.
[30] Ibid.
[31] Canadian Centre for Child Protection, 'How we are Failing Children: Changing the Paradigm', https://protectchildren.ca/en/resources-research/child-rights-framework.
[32] Ibid.
[33] Ibid.
[34] Ibid.

advertise where to find additional images or videos of child sexual abuse.[35] For these types of materials that are used as pointers to known CSE material, the eSafety Commissioner should have the power to demand the image or video be taken down even where the image or video does not itself constitute CSE material but is part of the lead up to such material.

4. Should the Act have strengthened and enforceable Basic Online Safety Expectations?

Yes, the Basic Online Safety Expectations should apply to the wider spectrum of services that the Online Content scheme applies to, and where appropriate the expectations should also be enforceable with penalties for not complying with them. We acknowledge that the eSafety Commissioner will need to apply discretion in determining if services are adequately meeting the expectations. That is no different to other regulators. For example, workplace occupational health and safety regulators need to determine if an employer has taken reasonable actions to provide a safe workplace. AUSTRAC needs to use its discretion to determine if a reporting entity under the *Anti-Money Laundering and Counter-Terrorism Financing Act* has taken reasonable steps to assess the risks of their services being used for money laundering and taken adequate action to address those risks.

We welcome the strengthening of the Basic Online Safety Expectations made through the recent *Online Safety (Basic Online Safety Expectations) Amendment Determination 2024.*

In addition, services that are covered by the Basic Online Safety Expectations should be required to have structures in place that allow users to easily report evidence of child exploitation material or activities on their platforms. Specifically, requirements should include:

- Reporting structures should allow for anonymous reports of illegal material to be made;
- The reporting structure should not require a person to have an account on the platform or have to log into the platform;
- The reporting tools should be easy to find on all the interfaces of the platform provider, including desktop and mobile versions of the platform; and
- It must be possible to report specific users, user profiles, specific posts, or a combination of the latter.

In a report released in late 2020, the Canadian Centre for Child Protection (CCCP) reported on the experience of survivors of child sexual abuse in trying to get images and videos of their abuse removed. They often faced exceedingly long delays in responding to them reporting images if their abuse, content moderators challenging survivors on the veracity of the material or the report of the abuse material being ignored.[36] Survivors reported that hosting platforms' ambiguous and non-specific reporting options were a key barrier to successfully getting images of child sexual abuse material removed.[37]

Additional barriers hosting platforms have put in place that hinders the removal of child sexual abuse material are:[38]

- Reporting structures that create strong disincentives for users to report illegal content, such as requirements to provide personal contact information;

[35] Canadian Centre for Child Protection, 'How we are failing children: Changing the paradigm', 2019, 8.
[36] Canadian Centre for Child Protection, 'Reviewing Child Sexual Abuse Material reporting functions on popular platforms', 2020, 7.
[37] Ibid., 7.
[38] Ibid., 8.

- The inability to report publicly visible content without first creating (or logging onto) an account on the platform;
- Difficulty locating reporting tools on the interface, with, at times, inconsistent navigation between desktop and mobile versions of the platform; and
- The inability to report specific users, user profiles, specific posts, or a combination of the latter.

The CCCP reported that WhatsApp and Skype delete chats of users reported for child sexual abuse activity, meaning complainants become unable to forward the chat to police.[39]

A tipline analyst, who works with social media platforms all the time, reported that it regularly took them 20 minutes to find places on the platforms where to report child sexual abuse material.[40] Thus, for ordinary people the time taken to find where to report such material is likely to be longer, acting as a barrier to reporting.

5. Should the Act provide greater flexibility around industry codes, including who can draft codes and the harms that can be addressed? How can the codes drafting process be improved?

Responsibility for drafting the industry codes and including the harms that can be addressed, should be the responsibility of the regulator, with input from people with lived experience of online safety harm and from industry representatives to point out genuine limitations or factors that need to be considered. The drafting process could be improved by requiring independent experts to lead the process.

6. To what extent should online safety be managed through a service providers' terms of use?

We note that the recent changes to the *Online Safety (Basic Online Safety Expectations) Determination 2022* provides a new additional expectation that service providers take reasonable steps, including proactive steps, to detect breaches of terms of use, policies and procedures, and standards of conduct. The Synods welcome that the change that sets the expectation that service providers should not rely solely on user reports and complaints to identify and address such material and activity that breaches its rules of conduct in relation to online safety.

7. Should regulatory obligations depend on a service providers' risk or reach?

We recommend that regulatory obligations should be based on the risk and reach of services, such as is in the EU and UK legislation.

Part 3 – Protecting those who have experienced or encountered online harms

8. Are the thresholds that are set for each complaints scheme appropriate?

The Synods believe that the existing thresholds for the complaints schemes need to be reformed.

[39] Ibid., 12.
[40] Michael Salter and W. K. Tim Wong, 'the impact of COVID-19 on the risk of online child sexual exploitation and the implications for child protection and policing', University of NSW, May 2021, 39.

In the case of child cyberbullying or adult cyber-abuse, a person being subjected to cyber-bullying by someone located in Australia or its territories should be able to make a complaint even if they are a usual resident overseas. There is a need to send a clear signal that it is unacceptable to cyber-bully anybody regardless of their location or nationality. The concern is particularly relevant with the rise in far-right racist extremism in Australia. The Director-General of ASIO told the Senate Legal and Constitutional Affairs Budget Estimates hearing on 20 October 2020 that right-wing extremists were more organised, sophisticated, ideological, and active than previous years. He stated that extreme right-wing individuals comprised 30 – 40% of ASIO's priority counter-terrorism investigative subjects in the 2019 – 2020 financial year.[41] He told the hearing that many of these people believe 'race war' is inevitable.[42] The Synod agrees with the eSafety Commissioner and the Australian Human Rights Commission in their joint media release that:[43]

> *Constant vigilance is required to condemn and address racism, whether online or off. Australia prides itself on being a safe and welcoming country that addresses issues of racism and takes each racist incident seriously.*

The statement should apply to all racist cyber-bullying where someone located in Australia is the perpetrator.

Complaints for image-based abuse, child cyberbullying and adult cyber-abuse should be able to be made by any third party. The eSafety Commissioner would be free to assess such complaints to determine if they warrant investigation. The Commissioner should seek to contact the target of the harmful activity to determine if they support the Commissioner taking action.

As discussed above in this submission, recently short statured Australians have said that their photos are increasingly being taken without consent and posted on "m****t spotting" social media groups[44]. People who have experienced this type of online harm have said they wanted the wider public to help in the fight against their abuse, to call this behaviour out when they see it and for businesses to play a role in calling it out, given many of the photos and videos were recorded inside restaurants, shopping centres, and gyms[45].

Complainants of child cyberbullying and adult cyber-abuse should not be required to make the complaint to the online platform first in order for the eSafety Commissioner to be able to issue a removal notice. As noted in the issues paper, some services may respond to the complainant with malice. Others may respond with a dismissive response, which could cause further distress to the complainant.

As an example of how services have pushed back against requests to remove harmful material, the Canadian Centre for Child Protection reported that some corporations that host content would use any

---

[41] https://www.asio.gov.au/publications/speeches-and-statements/senate-legal-and-constitutional-affairs-budget-estimates.html

[42] Ibid.

[43] Australian Human Rights Commission and eSafety Commissioner, 'New resources for victims of cyber abuse in diverse communities', Media Release, 26 June 2020.

[44] https://www.abc.net.au/news/2024-05-30/short-statured-community-call-out-online-abuse-facebook-groups/103896180 Short statured Australians are facing increased online abuse. They're asking for the public's help to stop it By the Specialist Reporting Team's Evan Young and Maryanne Taouk Posted Thu 30 May 2024 at 6:03am

[45] Ibid.

signs of physical maturity in images of victims of child sexual abuse as a reason not to remove a child sexual abuse image. The refusal to remove the image will be despite the request to remove the image coming from an expert on determining that the image is child sexual abuse.[46]

The Canadian Centre for Child Protection report that content host corporations will often dispute the removal of images of a child with what is likely to be semen on their face. The corporation will argue that they are not able to verify that the substance is semen.[47]

9. Are the complaints schemes accessible, easy to understand and effective for complainants? and

10. Does more need to be done to make sure vulnerable Australians at the highest risk of abuse have access to corrective action through the Act?

For complaints schemes to be effective for all people, people with disabilities require accessible information about complaints processes and accessible complaints processes including the use of interpreters, through reasonable adjustment if required. Recommendations from the final report of the Royal Commission into Violence, Abuse, Neglect and Exploitation of People with Disabilities (the Royal Commission) are relevant to the complaints schemes under the *Online Safety Act.* The Royal Commission recommended a national plan to promote accessible information and communications, along with an increase in Auslan interpreters. The Royal Commission also recommended that adult safeguarding functions with 'one-stop shop' complaint reporting, referral and support be available to facilitate complaints from people with disabilities in recognition of their vulnerability in reporting harm to agencies such as police services. In addition, the Royal Commission recommended that the Commonwealth Ombudsman should lead a co-design process with the NDIS Quality and Safeguards Commission, state and territory ombudsmen and other bodies with complaint handling and investigation expertise, to develop guidelines for organisations on implementing complaint handling systems that are accessible and responsive to people with disability. We support the recommendations presented below from the Royal Commission and recommend that the Australian Government implement these and include these in the way the eSafety Commissioner operates under the *Online Safety Act.*

People with disability could either make a complaint to the proposed independent 'one-stop-shop' that would refer the relevant complaints to the eSafety Commissioner or directly to the eSafety Commissioner.

Recommendation 6.1 A national plan to promote accessible information and communications
The Australian Government and state and territory governments should develop and agree on an Associated Plan in connection with Australia's Disability Strategy 2021–2031 to improve the accessibility of information and communications for people with disability. The Associated Plan should be co-designed with people with disability and their representative organisations. It should be finalised by the end of 2024.

The Associated Plan should:

[46] Canadian Centre for Child Protection, 'How we are Failing Children: Changing the Paradigm', https://protectchildren.ca/en/resources-research/child-rights-framework.
[47] Canadian Centre for Child Protection, 'How we are failing children: Changing the paradigm', 2019, 24.

- consolidate and build on existing initiatives and commitments by governments;
- recognise the diversity of people with disability and the many formats and languages that people may require information to be provided in;
- consider the roles of various stakeholders, including the Australian Government, state and territory governments, disability service providers, disability representative organisations and organisations representing people from culturally and linguistically diverse backgrounds;
- focus, in the first instance, on information and communications about preparing for and responding to emergencies and natural disasters, and public health;
- include targeted actions to ensure access to information and communications for people with disability in the criminal justice system; supported accommodation, including group homes; Australian Disability Enterprises; and day programs;
- identify and allocate appropriate funding and resources for delivery;
- include mechanisms for review and public reporting of progress made against the Associated Plan.

Recommendation 11.1 Nationally consistent adult safeguarding functions
States and territories should each:

- introduce legislation to establish nationally consistent adult safeguarding functions, including: definitions of 'adult with disability', 'violence', 'abuse', 'neglect', and 'exploitation'
- at a minimum, the principles, functions and powers outlined in Table 11.1.1
- data collection and public reporting, including demographic data (for example, relating to First Nations, culturally and linguistically diverse, and LGBTIQA+ people with disability)
- a mechanism to review the legislation after a reasonable period to examine its efficacy.

b. ensure adult safeguarding functions are operated by adequately resourced independent statutory bodies
c. develop a National Adult Safeguarding Framework led by the appointed adult safeguarding bodies
d. consider whether to co-locate the adult safeguarding function with the 'one-stop shop' independent complaint reporting, referral and support mechanism (see Recommendation 11.3).

Recommendation 11.2 An integrated national adult safeguarding framework
The Australian Government should incorporate the National Adult Safeguarding Framework proposed in Recommendation 11.1 into the Safety Targeted Action Plan within Australia's Disability Strategy or another suitable authorising document.

Recommendation 11.3 'One-stop shop' complaint reporting, referral and support
States and territories should each establish or maintain an independent 'one-stop shop' complaint reporting, referral and support mechanism to receive reports of violence, abuse, neglect and exploitation of people with disability. This mechanism should perform the following functions:
a. receive complaints or reports from anyone concerned about violence, abuse, neglect and exploitation involving a person with disability in any setting;
b. provide advice and information to people with disability, representative organisations and other interested parties about appropriate reporting options;
c. with a person's consent: make warm referrals to appropriate complaints bodies and make warm referrals to advocacy and other services who can support them in the complaint process
d. refer 'third party' reports to police, including anonymous reports;
e. collect, analyse and publicly report annual data on complaints and reports received and on referrals.

The mechanism should be co-designed with people with disability to ensure entry points are accessible to and effective for people with a range of abilities, language and communication needs.

The mechanism should be placed, if possible, within an existing independent organisation which has appropriate expertise and relationships with services to perform its functions.

Recommendation 11.4 Creating accessible complaint pathways
The Australian Government should work with states and territories to establish a national 1800 number, website and other accessible reporting tools to direct people to the independent complaint and referral mechanism in their state or territory.

Recommendation 11.5 Complaint handling and investigative practice guidelines
The Commonwealth Ombudsman should lead a co-design process with the NDIS Quality and Safeguards Commission, state and territory ombudsmen and other bodies with complaint handling and investigation expertise, to develop guidelines for organisations on implementing complaint handling systems that are accessible and responsive to people with disability. The guidelines should reflect the ten core components:
• creating a rights-focused complaints culture;
• encouraging people with disability and others to speak up;
• making adjustments to enable participation;
• supporting the person with disability, their family and others in complaint processes;
• respecting complexity, diversity and cultural difference;
• providing clear information about how to complain and multiple pathways to complain;
• working respectfully and effectively alongside police;
• conducting safe and inclusive investigations that are trauma-informed;
• providing tailored outcomes and redress;
• using complaints data to drive continuous improvement in service provision and complaint handling.

We note that the recent changes to the *Online Safety (Basic Online Safety Expectations) Determination 2022* include the new additional expectation (new subsection 14(3) of the Act) which provides that services should respond to reports and complaints within a 'reasonable period of time', that service providers will take reasonable steps to give feedback on the action taken, within a reasonable period of time[48]. Subsection 14(4) provides guidance about the factors that service providers should consider when determining what is a reasonable period of time to review, respond, and provide feedback in relation to the complaint or report[49].

We recommend that the Australian government reconsider the ethics and efficacy of requiring service providers to determine what is a 'reasonable period of time', and that the Australia government be the decision maker about what is a 'reasonable period of time', for example by providing timeframes for particular types of complaints and corrective actions.

Making such a requirement on what is a reasonable period of time is necessary due to online corporations having very different ethical standards. For example, consider the response of online

[48] Explanatory Memorandum.
[49] Ibid.

corporations to the hosting of child sexual abuse material. Corporations that host material online can be classed into five groups:[50]

- proactive, they actively seek to detect and prevent child sexual abuse imagery from being posted on their service;
- reactive, these corporations remove child sexual abuse material when they are notified that it is on their platform, but do not actively seek to prevent the posting of the material on their service;
- resistive, these corporations debate and push back against the removal of child sexual abuse material from their platform. They often dispute that the image is of a child or that it is illegal;
- non-compliant, these corporations ignore requests to remove child sexual abuse material from their service; and
- complicit, these corporations knowingly host child sexual abuse content and actively resist its removal as well as protecting people who post such material on their service.

At the 2019 eSafety conference in Sydney, the Canadian Centre for Child Protection (CCCP) reported that when they issue takedown notices for child sexual abuse material some content hosts do not prioritise the removal and others dispute removal. The CCCP said that on being issued with a notice to remove child sexual abuse material the time taken for content host companies to remove the content was:

- 10% within a day;
- 25% within two days;
- 50% within 3.5 days;
- The worst 25% within 11.5 days;
- The worst 10%, more than 25 days.

One content host took 360 days to remove an image of child sexual abuse once it was reported to them.

The Act currently does not include provisions relating to compensation and redress for victims of online harm. It is unclear whether victims of online harm are eligible for existing victim compensation or redress schemes. We recommend that the government review existing victim compensation and redress schemes, to address any gaps for victims in accessing compensation and redress for online harm.

11. Does the Commissioner have the right powers to address access to violent pornography?

If the violent pornography would fall into the refused classification category, then the appropriate response would be to have it removed or blocked from ready access. We note that it is very difficult to completely block access to online content from people very determined to access it.

Where the violent pornography would receive an R18+ classification, the solution would best be to require the content host and the pornography provider to ensure only adults are able to access the material. The eSafety Commissioner can only enforce such a requirement to the extent that there are requirements on the content host and pornography provider to implement such a measure and are required to use effective tools to achieve the outcome. Ideally, online users would have their identify verified, so their age would be known and would be able to provide such a verification to the content host or pornography provider. The identity would only be known to the entities that have had to verify their identity. They would remain anonymous to other users if that was their preference. The second best solution is some mechanism of age verification online. In both cases, there need to be in place

[50] Canadian Centre for Child Protection, 'How we are failing children: Changing the paradigm', 2019, 12.

safeguards to ensure that the identify information is securely stored and subject to unbreakable encryption, to avoid it being hackable by those that would seek to misuse it. Many online businesses appear to have to have been allowed to have inadequate levels of data protection and store people's identity information in accessible formats.

We would comment that we question the public interest served by violent pornography that would receive an R18+ classification. As noted in the issues paper, such material may cause harmful social impacts with distorted sexual attitudes and behaviours. We note that fictional material in film that deals with subjects of rape, sexual assault and family and domestic violence is often achieved within M and MA15+ categories.

12. What role should the Act play in helping to restrict children's access to age-inappropriate content (including through the application of age assurance)?

The Act should contain measures to help restrict children's access to age-inappropriate content. The extent of such measures depends on assessing their level of impact in providing additional safeguards for children to not access age-inappropriate content. Measures can have a beneficial outcome if they have a significant impact on reducing the prevalence of children accessing age-inappropriate content. Contrary to the views of some libertarian groups, measures do not have to be 100% effective to have a positive societal impact. Reducing inadvertent access can be of benefit, even if a determined teenager might be able to circumvent a safeguard.

The existence of tools and measures to circumvent safeguards does not mean that everyone will use them. For example, there are plenty of tools that perpetrators of online child sexual abuse can use to reduce the likelihood they will be caught by law enforcement, but many such offenders do not make use of such tools.

Given there are libertarian organisations already making suggestions that they would assist children in circumventing such safeguards about access to age-inappropriate content, it probably needs to be an offence for an individual or organisation to knowingly or recklessly instruct children on how to circumvent any safeguards put in place to restrict children's access to age-inappropriate content to deter deliberate undermining of any safeguards put in place.

13. Does the Commissioner have sufficient powers to address social media posts that boast about crimes or is something more needed?

The social media corporations should be required to make reasonable efforts to ensure that posts boasting about serious crimes are blocked from being posted and removed if they are posted. Such efforts should especially apply to crimes against people such a murder, rape, sexual assault, assault and family and domestic violence.

The Commissioner should have the power to issue a formal order to have such material removed, in addition to being able to make informal requests. The refusal or unreasonable delay in the removal of the material should result in penalties for the social media corporation.

There need to be safeguards to ensure that victims of crimes do not have posts unnecessarily removed, as these will not be boasting about the crime or encouraging further offending. However, we note such posts might be removed for other reasons. For example, a victim of a crime might make a post about the

crime but with a racist attack against all people from the assumed ethnic group of the alleged offender or encouraging vigilante violence.

14. Should the Act empower 'bystanders', or members of the general public who may not be directly affected by illegal or seriously harmful material, to report this material to the Commissioner?

As noted above, we support the Act empowering bystanders and members of general public being able to report harmful material to the Commissioner for assessment as to if an investigation and regulatory action are needed.

16. What more could be done to promote the safety of Australians online, including through research, educational resources and awareness raising?

Further research is needed to identify measures that will assist in preventing and deterring cyberbullying, cyber abuse, image-based abuse and child sexual abuse facilitated online. Further funding should be provided to the Australian Institute of Criminology for such work, given the impressive research they have conducted in the area. Additional research funds should be provided to the eSafety Commissioner as well as other researchers and research bodies conducting research that is likely to assist in identifying measures to make the online world a safer place.

Educational resources must be developed and awareness raising must be conducted about unauthorised use of photographs and videos that aren't 'indecent' but are being used without permission.

Part 4 - Penalties, and investigation and information gathering powers

17. Does the Act need stronger investigation, information gathering and enforcement powers?

To increase the effectiveness of the Act, additional investigation, information gathering and enforcement powers would be needed.

Investigations will continue to be hampered when abusive users of online services are able to have completely anonymous identities where no one knows who the real person is that owns the account. Relevant online providers should be required to have in place robust systems to verify the identity of the people using their service. Identity verification would allow law enforcement agencies, including the eSafety Commissioner, to increase the speed with which they can identify people suspected of being engaged in online criminal activity. It would also act as a general deterrent by reducing the perception of offenders they will not be identified for their online activities.

Not every online provider would be required to verify the identity of the person. For example, if the person has a Google account and Google has been required to verify the person's identity, providers that the person accesses via their Google account would not need to verify the person's identity as long as the service provider knows the person has accessed their service via Google and the person provides proof that Google knows who they are. If the person commits cyberbullying on the platform they have accessed from their Google account, the eSafety Commissioner should have the ability to go to Google and obtain the bully's identity.

Again, in the above system, the user would remain anonymous to other users if that was their preference, but at least one provider would know their identity.

Some aspects of internet psychology have been studied since the 1990s and are well known and documented. The effect of anonymity online – or perceived anonymity – is one example. It has been found to fuel online disinhibition, which is doing whatever you feel like, as you are not worried about the disapproval of others. Disinhibition is fed by the perceived lack of authority online, the sense of anonymity as well as the sense of distance or physical removal from others.[51]

Psychologist Jamil Zaki points out that anonymity tempts people to "try on cruelty like a mask, knowing it won't cost them. It does, of course, cost their targets."[52]

Due to the 'online disinhibition effect', as it is known, individuals can be bolder, less inhibited, and judgement impaired. Almost as if they were intoxicated. In this less-inhibited state, like-minded people can find one another quickly and easily, under a cloak of anonymity.[53]

The ease with which it is possible to set up multiple anonymous and false identities on social media platforms have greatly assisted those who seek to harm and abuse children online. Those who seek to abuse children online can pose as a child themselves and groom a child to develop a friendship or romantic relationship with the child.[54]

Example of how anonymous online identities assist in facilitating child sexual abuse

Alladin Lanim from Sarawak, Malaysia, had been sharing child sexual abuse material online since 2007. He was linked to more than 10,000 images and videos depicting the sexual abuse of children. He was able to hide behind an anonymous online profile. He was eventually identified in early 2021 and then located in July 2021. He was sentenced to 48 years in prison. Australian investigators identified 34 of the children he had abused, but there may be more.[55]

Being able to have anonymous identities online also assists child sexual abuse offenders in being able to assist each other, feeling that they can freely have conversations on online platforms and not be identified if the conversations were to be intercepted by law enforcement. There is increasing availability of products that help people conceal their online identities. Law enforcement agencies report that people involved in online child sexual abuse are increasingly using anonymising technologies, such as TOR and Virtual Private Networks (VPNs).[56] TOR and I2P assist those engaged in online child sexual abuse by randomly routing users' internet protocol (IP) traffic through other users' IP addresses. The process

[51] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 21.
[52] Jamil Zaki, 'The War for Kindness. Building Empathy in a Fractured World', Robinson, 2019, 148-149.
[53] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 5.
[54] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 14.
[55] Chris Barrett, 'How Australian police tracked one of the world's most wanted paedophiles to Borneo', *The Age,* 5 September 2021.
[56] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 5, 15.

assists child sex offenders from evading detection by law enforcement agencies.[57] TOR and VPNs are being built into some browsers by default.[58]

Those engaged in child sexual abuse online teach each other how to become anonymous online.[59] They are more commonly educating each other on using private chats, Internet voice and video chat software, forums and anonymisation software.[60] The feeling of impunity, because of those carrying out the abuse being able to conceal their identity, has enabled them to diversify their activities.[61]

Analysis of conversations between child sexual abuse offenders in forums on the dark web that were captured in February 2021 found:[62]

- 32.8% of conversations were about the use of social media platforms;
- 13.5% of conversations were about content storage and exchange;
- 10.4% were about the use of direct messaging;
- 7.4% were about secure operating systems;
- 6% on how to capture live footage when a child has been coerced into conducting a sexual act;
- 1.5% on cloud file sharing; and
- 1.5% on image management.

The analysis shows the importance social media plays in the activities of those engaged in online child sexual abuse, compared to other issues.

The eSafety Commissioner publicly raised concerns in July 2021 that the chat app Kik allowed people to be completely anonymous.[63] The app allowed people identified only by a username to share photos and videos. It also allowed them to video chat and find or form chat groups. Ramiz Adam was able to log into Kik using anonymous identities and share child sexual abuse material with more than 4,000 users. Kik stated on their website they would only comply with US judicial requests and only provide transaction chat logs. The company deleted all video and images after 30 days, destroying evidence of the sharing of child sexual abuse on its platform.[64]

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

The Synods believe that current penalties are inadequate given the level of harm that can result from non-cooperation by the online corporations and that some of the online corporations are enormous so that the existing maximum penalties would be regarded as a 'parking ticket'.

[57] Benoit Leclerc, Jacqueline Drew, Thomas Holt, Jesse Cale and Sara Singh, 'Child sexual abuse material on the darknet: A script analysis of how offenders operate', Australian Institute of Criminology, Trends & issues No. 627, May 2021, 2.
[58] WeProtect Global Alliance, 'Global Threat Assessment 2021', 27.
[59] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 15.
[60] Ibid., 16.
[61] Ibid., 5.
[62] WeProtect Global Alliance, 'Global Threat Assessment 2021', 28.
[63] Tessa Akerman, 'Paedophiles find prey in anonymous app', *The Australian,* 24 July 2021.
[64] Ibid.

The criminological literature indicates that for penalties to be effective, they need to be:[65]

- Proportionate
- Fair;
- Swift;
- Certain;
- Memorable;
- Cost effective; and,
- Incentivise and provide a pathway for the re-integration of the offender into compliance.

Memorable means that when a penalty is applied, it needs to be publicised to the broader body of reporting entities to provide greater general deterrence.[66]

Braithwaite argued that the 'trick' to successful regulation is to impose the fitting sanction as needed without undermining a regulator's capacity to persuade.[67] The greater the range of sanctions available to a regulator or law enforcement agency, the greater their ability to impose the right level of sanction. As Becker has argued, the desired outcome is to allow a regulator a penalty structure that optimally deters socially undesirable behaviour.[68]

Overly severe penalties can risk alienating the offender from the system and the law enforcement authority, which can negatively affect their compliance behaviour.[69] All penalties risk stigmatising those being penalised and pushing them further away from voluntarily complying, particularly if the people involved in being penalised feel they have been treated unfairly.[70]

Conversely, penalties that are too soft do not work as effective general or specific deterrence.[71] For example, Gregg Ritchie, one of KPMG's senior tax partners in the US, broke the law when he advised his firm not to register a tax shelter with the IRS. In a memo to colleagues, he stated, "Firstly, the financial exposure of the firm is minimal. Based on our analysis of the applicable penalty sections, we conclude that the penalties would be no greater than $14,000 per $100,000 in KPMG fees." He also argued it was simply the industry norm "There are no tax products marketed to individuals by our competitors which are registered."[72] He concluded:[73]

---

[65] Chris Leech, 'Detect and deter or catch and release: Are financial penalties an effective way to penalise deliberate tax evaders?', Tax and Transfer Policy Institute, Australian National University, Working Paper 6/2018, April 2018, 40.
[66] Ibid., 42.
[67] John Braithwaite, 'To Punish or Persuade: Enforcement of Coal Mine Safety', State University of New York Press, 1985, 117.
[68] Cindy Alexander and Mark Cohen, "Causes of Corporate Crime. An Economic Perspective", in Anthony Barkow and Rachel Barkow (eds.), "Prosecutors in Boardrooms", (New York University Press, 2011), 21.
[69] Chris Leech, 'Detect and deter or catch and release: Are financial penalties an effective way to penalise deliberate tax evaders?', Tax and Transfer Policy Institute, Australian National University, Working Paper 6/2018, April 2018, 40-41.
[70] Ibid., 43.
[71] Ibid., 41.
[72] Eugene Soltes, *Why they do it*, (USA: Public Affairs, 2016), 90.
[73] Ibid., 90.

> *Any financial exposure that may be applicable can easily be dealt with by setting up a reserve against fees collected. Given the relatively nominal amount of such potential penalties, the Firm's financial results should not be affected by this decision…. The rewards of successful marketing of [the tax structure] product (and the competitive disadvantages which may result from registration) far exceed the financial exposure to penalties that may arise.*

Meta-analysis of what works to deter businesses from breaking the law found that a combination of enforcement strategies worked best, rather than the over-reliance on just one approach.[74] A combination of law, regulatory policy and punitive sanctions was found to significantly deter businesses breaking the law.[75] The researchers concluded:[76]

> *It makes sense to focus on regulatory policies at the middle level of the [regulatory] pyramid where persuasion is generally most needed to achieve compliance. Specifically, our findings indicate that policies may be more successful when industry has some input and policies are coupled with education and consistent inspections. More severe strategies (regulatory investigations, penalties, civil suits and arrest/jail time) should be added where compliance has been difficult to achieve.*

Further:[77]

> *Results offer support for a model of corporate regulatory enforcement that blends cooperation with punishment –the type and amount of enforcement response to be determined by the behaviour of the manager/ company (i.e., responsive regulation). Thus, at the top and even middle levels of the enforcement pyramid, multiple "levers" may need to be pulled to achieve compliance.*

Given some online corporations have demonstrated resistance to compliance and cooperation with the eSafety Commissioner, we support that maximum penalties for non-compliance should be a portion of annual global turnover of the online corporation, so that the penalty is scaled to their size in line with other overseas jurisdictions. In addition, refusal to remove child sexual abuse material should also have a maximum fine of 50,000 penalty units and 100 penalty units for every day that the material remains online beyond the 24 hours that a formal removal notice required for the material to be removed. Other maximum penalties should be scaled based on the level of harm caused by the offence in question.

19. What more could be done to enforce action against service providers who do not comply, especially those based overseas?

And

20. Should the Commissioner have powers to impose other enforcement actions such as business disruption sanctions?

For large entities that have a presence in Australia, a solution would be to require the corporation to have staff in Australia who are responsible for compliance with the requirements of the Act. Where

[74] Schell-Busey, Natalie, Simpson, Sally, Rorie Melissa and Alper, Mariel, 'What Works? A Systematic Review of Corporate Crime Deterrence', *Criminology and Public Policy* Vol. 15 No. 2, 2016, 401.
[75] Ibid., 404.
[76] Ibid., 406.
[77] Ibid., 408.

there is non-compliance the individuals in Australia who have the power to ensure compliance should be individually subjected to penalties in addition to the penalties placed on the corporation they work for.

It has been recognised that where a corporation is fined, rather than the sanction falling on the individuals involved, the penalty fails to act as a general deterrent to the illegal behaviour. Associate Professor Soltes gives an example: [78]

> *For instance, the day after settling criminal charges with federal prosecutors for helping wealthy individuals evade taxes, executives at Credit Suisse held a conference call to reassure analysts that the criminal conviction would have "no impact on our bank licenses nor any material impact on our operational or business capabilities." And, ironically, fines levied on offending firms are ultimately paid by shareholders rather than by executives or employees who actually engaged in the misconduct. Without the spectre of the full justice system hanging over them, as is the case with individual defendants, labelling firms as criminal often has surprisingly weak, or even misdirected, effects.*

For smaller entities that do not have an Australian presence that can be held to account, the Australian Government should consider having Australian ISPs having to disrupt access to such entities. Such an approach has been adopted by the ACMA for online gambling providers that refuse to comply with Australian law.[79] If the eSafety Commissioner were granted such a power, the Commissioner would need to consider the impact on people who access the services of the entity before imposing the access disruption.

The use of other forms of business disruption sanctions would need to consider the possible harms to those that use the online service. For example, it could cut an individual off from their main source of communication with a loved one overseas or cause economic loss to an Australian business using the online service and has not itself engaged in any illegal behaviour.

Part 5 – International approaches to address online harms

21. Should the Act incorporate any of the international approaches specified above? If so, what should this look like?

The Australian *Online Safety Act* should maintain a hybrid approach, allowing for individuals to make complaints and for the eSafety Commissioner to take systemic action in relation to regulated entities, and should introduce a statutory duty to care approach based on the UK *Online Safety Act.*

22. Should Australia place additional statutory duties on online services to make online services safer and minimise online harms?

The Synods believe that online services should have statutory duties to ensure that they have implemented safety by design principles and 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. While the best interests of the child requirement was included in the *Online Safety (Basic Online Safety Expectations) Amendment Determination 2024,* we believe it should be an enforceable requirement to shift the culture of the online industry. The online services corporations have been allowed to develop

[78] Eugene Soltes, 'Why they do it', Public Affairs, USA, 2016, 325.
[79] https://www.acma.gov.au/blocked-gambling-websites

and grow with little consideration for the safety of the people using their products. Even worse than that, a number of whistleblowers that worked in senior positions in the online service corporations have reported that when safety and well-being considerations of users were in conflict with increasing profits, the desire for increased profits was usually given priority.

The requirements of having a statutory obligation to implement safety by design and acting in the best interests of children will need to be backed up by the eSafety Commissioner having the ability to provide protection from retaliation for whistleblowers that expose non-compliance with the obligations. These could be in line with the measures recently introduced for whistleblowers to the Tax Practitioners Board in the *Treasury Laws Amendment (Tax Accountability and Fairness) Act 2023.* In addition, whistleblowers should be able to access a financial reward in the form of a portion of any penalty paid as a result of the information they provided, as often whistleblowers will not be able to work in the same industry again and will need to change careers. Financial rewards can assist in that process.

Professor of Psychology at Rider University, John Suler, has said of letting children access the internet without restriction: "You wouldn't take your children and leave them alone in the middle of New York City, and that's effectively what you're doing when you allow them to go into cyberspace alone."[80]

Children are highly present on social media. Meta Platforms has a policy that no one below the age of 13 should have a Facebook page. Setting the minimum age for Facebook and Instagram at 13 years is a data-protection requirement by law in the US.[81] The US *Children's Online Privacy Protection Act 1998* required that corporations needed parental consent before collecting information about children under the age of 13.[82] Under the Act, parents can demand that the social media corporation remove the social media site of their child.[83] Between 2011 and 2014, a group EU Kids Online conducted a study looking at the online activities of children in 22 countries. They found that a quarter of nine and ten-year-olds had a Facebook page. Approximately half of 11 and 12-year olds had a Facebook page. Four in ten of these children provided a false age when setting up the page.[84] According to *Consumer Reports,* in 2011, there were 7.5 million children under the age of 13 that had Facebook pages.[85]

Meta Platforms has stated that children under the age of 13 are not allowed on Facebook or Instagram.[86] Under government scrutiny, from June to August 2021, Facebook removed over 600,000 accounts on Instagram that were unable to meet minimum age requirements.[87] Meta Platforms also announced that all users under the age of 16 in the US would be defaulted into a private account when they join Instagram.[88]

---

[80] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 121.
[81] Ibid., 125.
[82] https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Web%20sites%20and%20online
[83] Ibid.
[84] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 124-125.
[85] Ibid., 125.
[86] Antigone Davis, Global Head of Safety, Facebook, Hearing before the US Senate Committee on Science, Commerce, and Transportation, Subcommittee on Consumer Protection, Product Safety, and Data Security, 30 September 2021, 2.
[87] Ibid., 2.
[88] Ibid., 3.

Cyber psychologist Mary Aiken has pointed out that children aged four to 12 years old are the group most vulnerable to harm on the Internet as users. They are naturally curious and want to explore. They are old enough to be competent with technology. However, they are not old enough to be wary of the risks online. More importantly, they do not yet understand the consequences of their behaviour there.[89]

Police have pointed out that children online may not yet have the maturity, tools and skills to differentiate between online friendships and online sexual abuse.[90]

Online multiplayer games represent an example of where children can be vulnerable online due to a lack of safeguards built into the environment. When a child is playing an online multiplayer game, they are leaking vast amounts of information about themselves into cyberspace. Information that is useful to predators. The child's use of language can give away their age. The length of time the child plays uninterrupted can provide an indicator of parental supervision. How late the child can stay up can also hint how much parental supervision there is. What times the child is online will help locate where they are and what the family routine is.[91]

If a predator plays online with a child over time, they can figure out where the child lives. Eventually, they will be able to determine or estimate the child's level of social isolation. If the child is a loner, they are more likely to be vulnerable to approaches from the predator. The child's emotional stability can be judged by how they react to engineered scenarios in which they are put under pressure during the game – a way to test their resilience.[92] The predator will be able to see if the child is upset easily, if they are volatile or reckless. The predator will try to figure out if the child is home alone, or what time of day the parents are likely to be gone. All of this information is available to a potential predator before a one-on-one personal conversation begins with the child.[93]

A young child can be influenced, brought along slowly, by complimenting them on their exceptional playing style, giving them a support network, and asking them to join a permanent team in a multiplayer game. Sometimes predators hunt in packs and will have a team they invite the child into where they pretend they do not know each other.[94]

Individuals behave differently when part of a group than when they are alone. It has been proven that teenagers, in particular, can be judgement-impaired when in groups of peers, known as the risk-shift phenomenon. Teenagers in groups engage in riskier behaviour.[95] Large groups of teenagers online, connected by social networks, are likely to behave in riskier ways. They will also feel more peer pressure the larger their online social group is.[96]

Counter to safety by design, US law has assisted US social media corporations not taking responsibility for what is posted on their platforms. The US *Communications Decency Act of 1996* protects technology

[89] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 120-121.
[90] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 8.
[91] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 152.
[92] Ibid., 152.
[93] Ibid., 152-153.
[94] Ibid., 153.
[95] Ibid., 197.
[96] Ibid., 198.

corporations from any consequences of what is published on their platforms. They are not held responsible for the material on their platforms because they are not deemed a "publisher or speaker". [97]

23. Is the current level of transparency around decision-making by the industry and the Commissioner appropriate? If not, what improvements are needed?

The Australian Government should follow the lead of other jurisdictions and give the eSafety Commissioner powers to require providing requested information to the Commissioner, require the publication of online safety risk assessments and what mitigation measures have been taken by the entity, and mandatory audit requirements for large entities. The Australian Government should follow the lead of the UK Government and require service providers to publish children's risk assessments, as part of their overall risk assessment, and include what actions have been taken to address the identified risks.

The eSafety Commissioner should also have the power to hold hearings into all matters to make the online world safety and be able to require service providers to attend.

24. Should there be a mechanism I place to provide researchers and eSafety with access to data? Are there other things that they should be allowed to have access to?

The eSafety Commissioner should have the power to require large service providers to provide accredited researchers with access to data. Whether such a power should extend to smaller service providers depends on the public interest and safety benefit of researchers having access to such information against the cost imposition on the smaller provider in complying.

In addition to the information we have specified that the eSafety Commissioner should have access to in our answer to question 23, we support the eSafety Commissioner having a general power to have access to any information that the Commissioner reasonably assesses would assist in making the online world a safer place.

26. Are additional safeguards needed to ensure the Act upholds fundamental human rights and supporting principles?

The Synods agree with the discussion paper that in considering upholding human rights in the online space all relevant human rights need to be considered. Weighting should be given to addressing the human rights violations that create the greatest harm when these human rights are in conflict. For example, some impact on privacy rights are needed to ensure law enforcements agencies can protect children from online facilitated child sexual abuse and sexual extortion.

We note that there are libertarian advocacy groups who argue that privacy rights and freedom of expression online are the only rights that matter. Such groups, in their submissions to government inquiries, do not acknowledge child sexual abuse as a human rights violation referring to it only as a crime. However, such groups have also been inconsistent. Many of them opposed government efforts to require ISPs to disrupt ready access to images and videos of children who have been sexually abused, in opposition to the privacy rights of the victims/survivors of such abuse. The consistency in their position

[97] Harcher, P., 'Taming big tech's titans', *The Age*, 25 February 2020, 20.

have been constant opposition to any increase in the powers of law enforcement agencies to make the online world a safer place.

Part 6 – Regulating the online environment, technology and environmental changes

27. Should the Commissioner have powers to act against content targeting groups as well as individuals? What type of content would be regulated and how would this interact with the adult cyber-abuse and cyberbullying schemes?

Yes, the Commissioner should have powers to act against content targeting groups as well as individuals, for the same type of content that applies to individuals. The characteristics that should be protected from online hate should be aligned with protected characteristics in anti-discrimination legislation, including:

- Race;
- Ethnicity;
- Religion;
- Disability;
- Gender identity;
- Age;
- Association to a person with a disability;
- Sex;
- Pregnancy;
- Marital or relationship status; and,
- Sexual orientation.

Promotion of hatred for the above characteristics can cause real harm to the people targeted, which can reasonably be seen as a form of adult cyber abuse.

28. What considerations are important in balancing innovation, privacy, security, and safety?

Safety should always be the primary consideration, particularly safety obligations under international human rights instruments that Australia has ratified. Organisations that campaign against effective law enforcement tools to prevent online child sexual abuse and other severe online harms usually mount their arguments on the basis that the right to privacy overrides all other human rights, including those that require children to be protected from sexual abuse. Gail Kent from the Stanford Law School has pointed out the problem of providing too many safeguards over the right to user privacy at the expense of the human rights of victims, including survivors of child sexual abuse[98]:

> *There is frustration at an inability to get all communications data relating to nationals, including content, under their own national laws, especially where these laws have proven robust human rights safeguards not enhanced by duplicate processes. In many cases, double-checking does no more to protect the privacy of the user, instead frustrating the investigative or judicial process in the country requiring the information.*

[98] Gail Kent, 'The Mutual Legal Assistance problem explained', The Centre for Internet and Society, Stanford Law School, 23 February 2015,

In 2022, the House of Representatives Select Committee on Social Media and Online Safety concluded that while privacy concerns are critical to the rights of all internet users, those issues did not "outweigh the fundamental issue of ensuring safety in online environments"[99].

29. Should the Act address risks raised by specific technologies or remain technology neutral? How would the introduction of a statutory duty of care or Safety by Design obligations change your response?

Although the Act is technology-neutral, we note that the recent changes to the *Online Safety (Basic Online Safety Expectations) Determination 2022* address risks raised by specific technologies including the use by services of generative artificial intelligence (generative AI) and recommender systems. The new expectations applying to these technologies include the principles of safety by design and proactive minimisation of unlawful and harmful material or activity. The explanatory memorandum acknowledges that inclusion of these technologies recognises the increased risks of such technologies in adversely affecting online safety such as by enabling or amplifying the provision of unlawful or harmful material on a service[100]. This expectation applies to all stages of the development and deployment cycle or 'stack' of a product or capability, and it applies to all relevant electronic, designated internet, and social media services involved in the development and deployment of generative AI[101]. The obligation recognises that each service in this cycle has a role in ensuring that the final product made available to end-users promotes user safety[102].

A statutory duty of care and a requirement of Safety by Design would apply to all technology developments and place the obligation on the technology or product developers and operators to ensure that they have designed products and services that are as safe as reasonably possible for users and expressing appropriate care for the users of the products and services.

30. To what extent is the Act achieving its object of improving and promoting online safety for Australians?

The Act is only partially achieving its objectives of improving and promoting online safety. Some online service providers continue to interfere globally in upholding the safety and human rights of people online, including lobbying and advocacy against regulatory improvements. We have provided recommendations in this submission to improve and promote online safety.

31. What features of the Act are working well, or should be expanded?

The Synods believe that the *Online Safety Act* makes a valuable contribution to improving online safety for Australians, as demonstrated by the Commissioner having caused online service providers to improve the safety on their platforms and services and the number of cases that the eSafety Commissioner has been able to address in response to complaints made to the Commissioner. We have provided recommendations in answers to the questions above to improve and promote online safety.

[99] Parliament of the Commonwealth of Australia, House of Representatives Select Committee on Social Media and Online Safety, 'Social Media and Online Safety' March 2022.
[100] Explanatory Memorandum.
[101] Ibid.
[102] Ibid.

We believe that imposing a duty of care and Safety by Design principles on social media corporations is urgently needed to address their plans to implement end-to-end encryption on their platforms in a way that will currently facilitate an increase in online child sexual abuse and other harms on their platforms.

A Safety by Design and duty of care approach to implementing end-to-end encryption in our view would:

- Enable law enforcement to obtain lawful access to content in a readable and usable format;
- Require social media corporations to engage in consultation with governments 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 thoroughly tested and operational.

32. Does Australia have the appropriate governance structures in place to administer Australia's online safety laws?

We believe that Australia has the appropriate governance structures in place to administer Australia's online safety laws.

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

Yes, Australia should introduce a cost recovery mechanism on online service providers for regulating online safety functions, as some online service providers continue to object to enforcement action in order to protect children and adults from online harm. The cost recovery mechanism should be developed according to the Australian Government Cost Recovery Policy and Guidelines. There is a need to ensure that the cost recovery model is designed in such a way that the online service providers are not able to influence the eSafety Commissioner by virtue of their funding of the Commissioner.

Rev. Bruce Moore
Moderator
Uniting Church in Australia
Queensland Synod
[redacted]

Dr Mark Zirnsak
Senior Social Justice Advocate
Uniting Church in Australia
Synod of Victoria and Tasmania
[redacted]