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

Centre for Theology and Ministry
[redacted]

Director
Online Safety Reform and Research Section
Department of Infrastructure, Transport, Regional Development and Communications
[redacted]
E-mail: OnlineSafety@infrastructure.gov.au

Submission by the Synod of Victoria and Tasmania, Uniting Church in Australia to the consultation on the Online Safety (Basic Online Safety Expectations) Determination 2021
12 November 2021

The Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes this opportunity to make a submission to the consultation on the *Online Safety (Basic Online Safety Expectations) Determination 2021*. The Synod supports the Basic Online Safety Expectations as drafted, with the comments below on where we believe they could be further strengthened.

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

The willingness of technology providers to assist or obstruct law enforcement agencies in combating child exploitation varies significantly. While some technology providers actively assist law enforcement to addressing child exploitation on their platforms, others actively hinder, delay and obstruct law enforcement efforts. Some do both at the same time.

As pointed out by Professor Alan Rozenshtein, these corporations hold a large degree of discretion when processing requests from law enforcement agencies. They can use discretion to slow down the processing of requests by insisting on proceduralism and minimising their capacity to respond to legal requests by implementing encryption.[1]

This discretion means these corporations determine, at least in part, government agencies access to information about our personal relationships, professional engagements, travel patterns and financial circumstances. At the same time, they impact the government's ability to prevent terrorism, the rape of children, solve murders and locate missing children. These corporations are now responsible for decisions that have significant consequences for our privacy on the one hand, and our safety and well-being on the other.[2]

[1] 'Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance', *Developments in Law – More Data, More Problems,* 131 Harvard Law Review (2018), 1715-1722.
[2] Ibid.

"From its earliest days, the internet has been weaponised against children around the world. From its earliest days, the technology sector has been negligent in ensuring that their platforms are not used to post child sexual abuse images. From its earliest days, the technology sector has profited while turning a blind eye to the horrific action of millions of their users around the world. This shameful behaviour must end. We must reclaim our online communities and hold the technology sector responsible for their actions and lack of action."[3]
Professor Hany Farid, Electrical Engineering & Computer Sciences and the School of Information, University of California

"During my time at Facebook, first working as the lead product manager for Civic Misinformation and later on Counter-Espionage, I saw Facebook repeatedly encountered conflicts between its own profits and our safety. Facebook consistently resolved these conflicts in favour of its own profits."[4]
Frances Haugen, 4 October 2021

"The Internet has been and will probably always be a wild, wild west in the minds of many people – a place where a badge is used for target practice. I believe it has something to do with the intrinsic design of the Internet."[5]
Professor John Suler, Department of Psychology, Rider University

"Platforms and algorithms that promised to improve our lives can actually magnify our worst human tendencies, Rogue actors and even governments have taken advantage of user trust to deepen divisions, incite violence, and even undermine our shared sense of what is true and what is false. This crisis is real. It is not imagined or exaggerated or "crazy"."[6]
Tim Cook, CEO, Apple

1. Recommendations

The Synod makes the following recommendations to strengthen the Basic Online Safety Expectations:

- Division 4 of *Online Safety (Basic Online Safety Expectations) Determination* 2021should be strengthened to ensure service users are easily report evidence of human rights abuses and criminal activity, including child exploitation material or activities on the service 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

[3] Canadian Centre for Child Protection, 'How we are failing children: Changing the paradigm', 2019, 3.
[4] Frances Haugen, 'Statement to US Senate Committee on Commerce, Science and Transportation, Sub-Committee on Consumer Protection, Product Safety and Data Security', 4 October 2021, 2.
[5] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 307.
[6] John Evans, 'Complete transcript, video of Apple CEO Tim Cook's EU privacy speech', Computerworld, 24 October 2018, https://www.computerworld.com/article/3315623/complete-transcript-video-of-apple-ceo-tim-cooks-eu-privacy-speech.html

    - It must be possible to report specific users, user profiles, specific posts, or a combination of the latter.
- Section 9 should be strengthened so that service providers 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 to increase the speed with which they can identify people suspected of being engaged in human rights abuses and criminal activity, including online child sexual abuse. It would also act as a general deterrent by reducing the perception of offenders they will not be identified for their online activities.
- The *Online Safety (Basic Online Safety Expectations) Determination* 2021should have an additional requirement that a service provider must preserve and report evidence of serious criminal activity, including child exploitation, on their platform to law enforcement agencies where an Australian victim or offender is involved.

Table of Contents

2. Uniting Church positions on regulating the online world

The meeting of the hundreds of Uniting Church representatives from across the congregations of the Synod in Victoria and Tasmania in 2011 adopted the following resolution regarding the regulation of the online world. It called on the Federal Government to adopt measures to deter online child sexual abuse, increase its detection and resource police to address all cases where Australians are involved in online child sexual abuse:

11.6.18.2.4 The Synod resolved:

(a) *To call on the Federal Government to adequately resource the Australian Federal Police to investigate all cases of online child sexual abuse where either the perpetrator or the victim is Australian;*

(b) *To call on the Federal Government to require Internet Service Providers (ISPs) to take action to assist in combating the sale, transmission and accessing of child sexual abuse images, which are always produced through human trafficking, forced labour, slavery or other means of manipulation and coercion. To that end, the Federal Government is requested :*

- *To leave the IT industry in no doubt that they have a legal obligation to report clients accessing child sexual abuse material when they detect it, regardless of privacy legislation; and*
- *To legislate to require ISPs to block client access to all websites that contain material classified as 'Refused Classification', regardless of where such sites are hosted, and to log attempts by clients to access child sexual abuse sites and provide this information to the authorities for investigation.*

The Synod meeting of congregation representatives in February 2021 passed the following resolution:

The Synod acknowledges:
The gospel calls us to relate to each other with love, treating each other with dignity and respect, and to condemn exploitation and abuse of vulnerable people. God's people are called to pursue justice including by empowering those who are exploited and abused.

The covenanting relationship between the Uniting Church in Australia and the UAICC, as we pursue justice together.

In our age, there is a need to prevent and address human rights abuses online, including acting against the promotion and facilitation of child sexual abuse.

It is the role of Parliament, through the laws it passes, to provide the framework for how law enforcement agencies and the courts can access information and people's communication online. This is not a role for technology corporations.

The Synod resolved:
(a) To commend the Commonwealth Government for their preparedness to act to make the online world a safer place for everyone.
(b) To call on the Commonwealth Government to ensure that the laws governing social media and the online world give law enforcement agencies the tools and budgets they need to prevent and address harms online. Such laws need to:

1. *Be effective and expedient to maximise the number of cases of harm that can be*

prevented and to ensure that evidence is not destroyed

2. *Provide appropriate protections for the privacy of people not engaged in inflicting harm on others or criminal activity without undermining the ability of law enforcement agencies to address serious online harms;*
3. *Provide thorough oversight and transparency on how law enforcement agencies use the powers they are provided with; and*
4. *Provide adequate sanctions to deter any misuse of powers granted to law enforcement agents*

(c) To commend the Commonwealth Government for its resourcing of the e-Safety Commissioner to educate the community about online safety.

(d) To call on the Commonwealth Government to ensure Australian law enforcement agencies work effectively with overseas law enforcement agencies to investigate and gather evidence of child sexual exploitation that have partly or wholly taken place in Australia or involving Australian residents.

(e) To call on the Commonwealth Government to ensure Australian law enforcement agencies take reasonable steps to guarantee information provided to overseas law enforcement agencies will not itself be used to perpetrate human rights abuses.

3. Enhancements to strengthen the *Online Safety (Basic Online Safety Expectations) Determination 2021*

> *"Facebook's regulators can see some of the problems – but they are kept blind to what is causing them and thus can't craft specific solutions. They cannot even access the company's own data on product safety, much less conduct an independent audit. How is the public supposed to assess if Facebook is resolving conflicts of interest in a way that is aligned with the public good if it has no visibility and no context into how Facebook really operates."*[7]
> Frances Haugen, 4 October 2021

3.1 Encrypted Services

The Synod strongly welcomes section 8, the additional expectation for providers regarding encrypted services. The Synod is deeply concerned that the increasing use of encrypted services is increasing the prevalence of human rights abuses facilitated online.

The increasing use of encryption is limiting the ability of police to investigate online child sexual abuse.[8]

The US National Center for Missing and Exploited Children has reported an increasing number of reports of online child sexual abuse material in the period 2014 - 2020, as shown in Table 1. However, it is not clear how much of the increase in reports is due to a rise in the amount of online child sexual abuse material. Some of the growth in reports may be due to better detection and reporting of such content. There was a decrease in the number of reports in 2019, before a massive increase in 2020.

Table 1. The number of reports of online child sexual abuse material reported to the US National Centre for Missing and Exploited Children 2014-2020.[9]

Year	2014	2015	2016	2017	2018	2019	2020
Number of reports of online child sexual abuse material (millions)	1.1	4.4	8.3	10.2	18.4	16.9	21.7

In 2019, Facebook made 15.9 million (94%) of the reports to the US National Center for Missing and Exploited Children.[10] Google provided 449,283 of the reports (2.7%).[11] Only 150,667 reports

[7] Frances Haugen, 'Statement to US Senate Committee on Commerce, Science and Transportation, Sub-Committee on Consumer Protection, Product Safety and Data Security', 4 October 2021, 3.
[8] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 6.
[9] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 9; US National Center for Missing and Exploited Children, '2019 Reports by Electronic Service Providers (ESP)', 2020; and US National Centre for Missing and Exploited Children, '2020 Reports by Electronic Service Providers (ESPs)', 2021.
[10] US National Center for Missing and Exploited Children, '2019 Reports by Electronic Service Providers (ESP)', 2020, 2.
[11] Ibid., 2.

(0.89%) of online child sexual abuse reported to the US National Center for Missing and Exploited Children came from members of the public.[12]

In 2020, Facebook made 20.3 million (94%) of the reports to the US National Center for Missing and Exploited Children.[13] Google provided 546,704 of the reports (2.5%).[14] The number of reports from the public increased to 303,299 (1.39%).

Facebook plans to implement end-to-end encryption on all its message services. In the UK alone, reports of suspected child sexual abuse posts and messages to law enforcement agencies by Facebook in 2018 resulted in 3,000 children being safeguarded from further child sexual abuse and the arrest of 2,500 suspected perpetrators.[15] If Facebook implements end-to-end encryption on all its message services it is estimated there will be a 70% drop in Facebook detecting cases of child sexual abuse.[16]

If end-to-end encryption is widely adopted, especially by Facebook, the US National Center for Missing and Exploited Children expect that the number of reports it will receive will halve, resulting in the abuse of tens of thousands of children going undetected.[17]

The Virtual Global Taskforce has pointed out that currently almost all reports of suspected online child sexual abuse material made by ICT corporations is detected by the use of artificial intelligence software.[18] No person from the corporation views the content before it is reported. Human content managers generally only view material following a report from a user who is a victim or witness to child sexual abuse, or following AI indicators which meet a high threshold for human moderation. The Taskforce has raised concern that end-to-end encryption is designed to prevent anyone from being able to access user content. The result will be that online child sexual abuse will only be able to be detected by the corporation providing the end-to-end encrypted communication using artificial intelligence to detect behavioural indicators through metadata. While much can be deduced from metadata, it is usually insufficient to meet the threshold required for a search warrant. Furthermore, the corporations themselves have advised that often individuals identified through behavioural indictors in their metadata only meet the policy threshold of the corporation to warrant a warning or exclusion from some features on the platform. The detected behaviour will often not generate a report to law enforcement agencies. The Virtual Global Taskforce points out that end-to-end encryption creates a risk that the corporations are unable to adequately safeguard children using their service. The lack of safeguarding occurs because they do not have enough information regarding online behaviours to warrant sharing referrals on potential abuse with law enforcement agencies. The Taskforce rightly points out that end-to-end encryption places the right to privacy of people producing and distributing child sexual abuse material over the right to privacy of their victims who should not

[12] US National Center for Missing and Exploited Children, https://www.missingkids.org/footer/media/keyfacts
[13] US National Centre for Missing and Exploited Children, '2020 Reports by Electronic Service Providers (ESPs)', 2021, 2.
[14] Ibid., 2.
[15] Letter organised by the UK National Society for the Prevention of Cruelty to Children signed by 129 children's rights organisations to Mark Zuckerberg, CEO, Facebook, 6 February 2020.
[16] Ibid.
[17] US National Center for Missing and Exploited Children, 'NCMEC's Statement Regarding End-to-End Encryption', 10 March 2019, https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption
[18] Virtual Global Taskforce position on End-to-End Encryption

have their images shared.

In a positive step, on 5 August 2021, Apple announced it was planning on scanning US iPhones for images of child sexual abuse. The Apple tool "neuralMatch" will detect known images of child sexual abuse without decrypting people's messages. If it finds a match, the image will be reviewed by a content manager who will report it to law enforcement agencies if necessary.[19] However, it is concerning that Apple will allow users to appeal to Apple against their assessment.[20] It should not be the role of Apple to tip off suspected child sexual abuse offenders that their activities have been detected. It should also not be for Apple to sit in judgement if a user has committed child sexual abuse offences.

3.2 Anonymous Identities

The Synod urges that section 9 should be strengthened. Ideally, no service provider should be permitted to allow a person to have an online identity where the provider does not know who the natural person who is using the online identity is. It is fine for a person to be able to conceal their identity from other users, but the provider should be required to know who the natural person is. Currently, where a person is using their online presence to commit human rights abuses or criminal acts and the provider does not know who the person is, the person can persist in their abusive or criminal activities for longer while law enforcement agencies try to identify them.

The ease with which it is possible to set up multiple anonymous and false identities have greatly assisted those who seek to 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. Having established the relationship, the child is then manipulated into sharing sexually explicit images of themselves with the abuser.[21] The material shared is then used to blackmail more sexually explicit material, under threat of the material being shared with the child's friends or family.[22]

Child sexual abuse perpetrators operate in networks online to assist each other.[23] The anonymity that technology corporations allow online has permitted thousands of people to be part of such networks. The Virtual Global Taskforce online child sexual exploitation assessment of 2019 reported an increase in the number of organised forums and groups of offenders online in the preceding three years.[24]

---

[19] Barbara Ortutay and Frank Bajak, 'Apple to scan US phones for child abuse images', *The New Daily,* 6 August 2021; and Reed Albergotti, 'Apple to scan phones for child pornography, sexual messages to minors', *The Australian Financial Review,* 7 August 2021.
[20] Reed Albergotti, 'Apple to scan phones for child pornography, sexual messages to minors', *The Australian Financial Review,* 7 August 2021.
[21] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 14.
[22] Ibid., 14.
[23] 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, 7.
[24] Ibid., 15.

Those engaged in child sexual abuse online teach each other how to become anonymous online.[25] They commonly educate each other on using private chats, Internet voice and video chat software, forums and anonymisation software.[26] Being able to conceal their identity, has allowed those carrying out the abuse feel a sense of impunity, enabling them to diversify their abusive activities.[27]

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).[28] TOR and I2P (the Invisible Internet Project) assist those engaged in online child sexual abuse by randomly routing users' internet protocol (IP) traffic through other users' IP addresses. The process assists child sex offenders from evading detection by law enforcement agencies.[29]

Criminological research has shown that once a penalty reaches a certain adequate level, then the risk of being caught has far more impact on whether a person will be deterred from committing a crime. The literature on crime finds that perceived certainty of punishment is associated with reduced intended offending.[30] The conclusion is that certainty of apprehension and not the severity of the legal consequences ensuing from apprehension is the more effective general deterrent.[31]

In the online world, there are tens of thousands of people engaged in dangerous criminal activity that harms other people at every moment in time. The more we allow people to have anonymous identities online, where nobody knows who the real person behind the online identity is, the harder and harder it becomes for police to catch such people. Further, when we allow technology corporations to destroy or conceal evidence of serious crimes, the less likely it is for people to be caught. The combination of completely anonymous identities, communication channels that police cannot access in any circumstances and technology corporations being able to conceal and destroy evidence of serious crimes creates an online environment where those wishing to harm others can have a sense of impunity. This encourages higher levels of severe criminal behaviour. The increased levels of serious criminal behaviour mean police can deal with a shrinking percentage of the online criminal behaviour with their finite resources, which in turn increases the number of people engaged in severe criminal behaviour. It becomes a vicious circle.

For general deterrence to work, people tempted to engage in severe criminal behaviour online must be given a sense that if they do so, they will be caught.

---

[25] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 15.
[26] Ibid., 16.
[27] Ibid., 5.
[28] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 5, 15.
[29] 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.
[30] Daniel S Nagin, 'Deterrence in the Twenty-First Century', *Crime and Justice* Vol. 42, No. 1, (August 2013), 201.
[31] Ibid., 202.

The sheer scale of the harms occurring online make traditional police techniques of investigating individual cases ineffective. Globally, police have reported that they are unable to adequately handle the volume of cases of online child sexual abuse they know of.[32] Effective policing online requires tools that allow for mass detection of serious criminal behaviour. Effective policing of the online world also requires disruption tools and techniques, things designed to make it harder to carry out criminal activity and get away with it or reduce its profitability. These tools provide greater deterrence for people who would otherwise succumb to the temptation to engage in criminal activity online.

The lack of effort to verify identities of service users also means large number of children are present in unsafe online environments. For example, Facebook 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.[33] 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.[34] Under the Act, parents can demand that the social media corporation remove the social media site of their child.[35] Between 2011 and 2014, the 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.[36] According to *Consumer Reports,* in 2011, there were 7.5 million children under the age of 13 that had Facebook pages.[37]

The lack of identity verification also has meant that child sexual abuse perpetrators can set up multiple Facebook accounts, pretending to be children themselves. These profiles are then used for activities like grooming and sexual extortion, with a vast pool of potential victims to prey on.

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.[38]

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.[39]

---

[32] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 11; and 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.
[33] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 125.
[34] https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Web%20sites%20and%20online
[35] https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Web%20sites%20and%20online
[36] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 124-125.
[37] Ibid., 125.
[38] Ibid., 120-121.
[39] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 8.

Facebook has stated that children under the age of 13 are not allowed on Facebook or Instagram.[40] Under government scrutiny, from June to August 2021, Facebook removed over 600,000 accounts on Instagram that were unable to meet minimum age requirements.[41] Facebook also announced that all users under the age of 16 in the US will be defaulted into a private account when they join Instagram.[42]

3.3 Complaints Process

The Synod believes that Division 4 regarding complaints needs to be strengthened, given the identified deficiencies in existing complaints mechanisms that service providers have in place.

> *From infancy until I was 15, I was trafficked and used in child sexual abuse material which continues to be shared widely across the internet. I spent hours every day searching for my own content, reporting thousands of accounts and posts sharing CSAM [Child Sexual Abuse Material]. When platforms don't actively look for or prevent this content from being uploaded, the burden falls to me to have these images removed. Each time one account gets taken down, five more like it take its place. It's like a hydra, a monster that I can never defeat. I'm not strong enough to take it down myself. It's costing me my well-being, safety and maybe even my life. I'm tired. I shouldn't find photos of myself as a child being raped when I'm just scrolling through my feed.*
> Survivor of child sexual abuse.[43]

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 lodging complaints to try 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.[44] 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.[45]

Additional barriers hosting platforms have put in place that hinders the removal of child sexual abuse material are:[46]

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

[40] 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.
[41] Ibid., 2.
[42] Ibid., 3.
[43] Canadian Centre for Child Protection, 'Reviewing Child Sexual Abuse Material reporting functions on popular platforms', 2020, 6.
[44] Canadian Centre for Child Protection, 'Reviewing Child Sexual Abuse Material reporting functions on popular platforms', 2020, 7.
[45] Ibid., 7.
[46] Ibid., 8.

- 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.[47]

3.4 Destruction of evidence by Service Providers

The 2018 documentary, 'The Cleaners', exposed how service providers are exploiting people in the Philippines to screen social media and remove abusive material, including child sexual abuse material. These people reported they are expected to look at up to 25,000 images a day. They alleged they get inadequate psychological support for being exposed to images of the worst depravity human beings are capable of. They also reported destroying the online evidence of child sexual abuse without referring it to the police. Such action could destroy vital evidence that could assist police in rescuing children from on-going abuse.

Thus, the *Online Safety (Basic Online Safety Expectations) Determination* 2021should have an additional requirement that a service provider must preserve and report evidence of serious criminal activity, including child exploitation, on their platform to law enforcement agencies where an Australian victim or offender is involved.

[47] Ibid., 12.

4. Online Child Exploitation

One of the significant reasons for the *Online Safety (Basic Online Safety Expectations) Determination 2021* is the prevalence of human rights abuses online, including child exploitation. Research and the experience of law enforcement agencies demonstrates that criminals are engaged in the rape, torture and sexual abuse of children of all ages facilitated by online platforms. They trade in images, videos or stream such horrific activity. They respond to both the opportunities new technologies provide as well as adapting to law enforcement strategies. It tends to be the least intelligent and least adaptive perpetrators that will be easiest for law enforcement to apprehend.

The children's rights network Terre des Hommes estimated that there will be roughly 750,000 men worldwide looking for online sex with children at any time of the day.[48]

Project Arachnid is a technological tool designed to reduce the availability of child sexual abuse images online.[49] Project Arachnid detects child sexual abuse material online by 'crawling' URLs across the global web known to have previously hosted child sexual abuse material. It makes the determination by comparing the media displayed on the URL to a database of known signatures that have been assessed by analysts as child sexual abuse material. If child sexual abuse material is detected, a notice is sent to the hosting provider asking for its removal.

Every month, Project Arachnid detects more than 500,000 unique images of suspected child sexual abuse material requiring analyst assessment. As of June 2019, those organisations running Project Arachnid had sent more than 3.6 million notices for removal of child sexual abuse material to online providers.[50] As of 4 August 2021, over 129 billion images had been assessed by Project Arachnid and over 40 million had been referred to analysts for review to determine if the image was child sexual abuse material.[51] Over eight million notices had been sent to content hosts to remove child sexual abuse material. Approximately 85% of these notices related to victims who were not known to have been identified by police.[52]

As of August 2017, the Internet Child Sexual Exploitation Database contained over one million unique images and videos.[53] Only a small fraction of the children captured in this material have been identified. Globally, law enforcement agencies have only been able to identify 19,100 of the children depicted in child sexual abuse material online.[54]

Online child sexual abuse remains a serious global problem in which thousands of Australians access, share, distribute and trade in child sexual abuse material. The Australian Institute of

[48] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 142; and Canadian Centre for Child Protection, 'Australia's hotline joins global project combating online child abuse', Media release, 5 June 2019.
[49] Canadian Centre for Child Protection, 'Australia's hotline joins global project combating online child abuse', Media release, 5 June 2019.
[50] Ibid.
[51] https://projectarachnid.ca/en/
[52] Ibid.
[53] Canadian Centre for Child Protection, 'How we are failing children: Changing the paradigm', 2019, 14.
[54] US National Center for Missing and Exploited Children, https://www.missingkids.org/footer/media/keyfacts

Criminology has reported that 256 detected Australians were suspected of having spent more than $1.3 million to pay for live-streaming child sexual abuse and rape from the Philippines.[55] Further, the 256 are only those Australians that have been detected and suspected of engaging in this abhorrent behaviour. The real total is undoubtedly much higher. The Philippines authorities have reported over a 250% increase in reported online child sexual abuse during the COVID-19 pandemic, with 279,166 cases reported in the period 1 March 2020 to 24 May 2020.[56] The number of suspicious transaction reports to the Philippines Anti-Money Laundering Council related to suspected online child sexual exploitation increase by 92% in the first half of 2020, from 10,633 in 2019 to 20,448 in the first half of 2020.[57] In part, the increase has been driven by greater compliance with reporting suspicious transactions by money service businesses in the Philippines.[58]

The Australian Institute of Criminology considered the 256 individuals based on those Australians that had interacted with 118 people arrested in the Philippines for facilitating the sexual abuse of children.[59] Of the 256 Australians identified, 21 had made between 21 and 141 financial transactions with the people arrested in the Philippines between January 2006 and February 2019.[60] These 21 suspected offenders spent a median amount of $75 per transaction. The median number of days between transactions was seven.[61] Twelve of the 21 suspected offenders had a prior criminal history.[62] However, only one of these had a previous history of sexual offences against children.[63]

The UK Internet Watch Foundation reported that in 2017 they detected 78,589 URLs containing child sexual abuse imagery up from 13,182 URLs hosting child sexual abuse material in 2013.[64] There was also an increase in the number of individual images of children being hosted, with 293,818 images being viewed.[65] In 2018, the Internet Watch Foundation removed 105,047 webpages showing sexual abuse and sexual torture of children.[66]

Dr Mark Zirnsak
Senior Social Justice Advocate
Phone: 0409 166 915
E-mail: mark.zirnsak@victas.uca.org.au

---

[55] Simon Benson, 'Agencies link 256 to online child sex', *The Australian*, 19 February 2020, 1.
[56] Republic of the Philippines Anti-Money Laundering Council, 'Online Sexual Exploitation of Children', 2020, 5, 8.
[57] Ibid., 11.
[58] Ibid., 11.
[59] Timothy Cubitt, Sarah Napier and Rick Brown, 'Predicting prolific live streaming of child sexual abuse', Australian Institute of Criminology, Trends and issues, No. 634, August 2021, 3.
[60] Ibid., 3-4.
[61] Ibid., 6.
[62] Ibid., 6.
[63] Ibid., 8.
[64] Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', 15; and Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', 6, 17.
[65] Internet Watch Foundation, 'IWF Annual Report 2016', 6.
[66] Internet Watch Foundation, 'Record number of images showing children being sexually abused removed by UK internet charity', 23 January 2019.