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

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

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

Submission by the Synod of Victoria and Tasmania, Uniting Church in Australia to the inquiry into law enforcement capabilities in relation to child exploitation
20 August 2021

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

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

1. Recommendations

The Synod requests that the Committee make the following recommendations:

- Australian law makes it an unambiguous offence for a technology provider not to preserve and report evidence of child exploitation on their platform to law enforcement agencies where an Australian child or offender is involved or where the provider is located in Australia.
- Legislation be passed by Parliament requiring technology providers 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.
- Technology 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 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.

- Prohibit social media corporations from allowing children under the age of 13 to open accounts on their platforms without verified parental or guardian consent.
- Existing legislation be reviewed and amended to ensure that individuals inside technology corporations can be prosecuted for refusing to co-operate with legislative requirements that assist in the investigation or prosecution of online child sexual abuse. The individuals in question should be those that make the decision not to co-operate.
- The Parliament pass the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* after the Government responds to the recommendations of the Parliamentary Joint Committee on Intelligence and Security.

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

Table of Contents

2. Uniting Church positions on tackling child sexual abuse

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.*

The Synod of Victoria and Tasmania has four resolutions from its delegates' meetings explicitly addressing child sexual abuse. The first is from 1993 and urges the Victorian Government to adopt measures to prevent the sexual abuse of women and children and to assist survivors of sexual abuse.

The second is from 1994 and called on the Victorian Government to take a holistic response to child sexual abuse in the community.

The third is from 2011 and explicitly addressed online child sexual abuse. 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 final resolution was adopted by the Synod meeting of congregation representatives in February 2021:

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. Human Rights Considerations

UN bodies are divided on where the balance lies between governments' need to protect people from online human rights abuses and the need for governments to protect online privacy generally. However, the vast majority stress the international human rights instruments require governments to prevent online child sexual abuse over the right to privacy of users of online systems when these rights are in conflict.

UN bodies that argue governments must effectively protect children from sexual abuse are the UN Office on Drugs and Crimes (UNODC), UNICEF, UNESCO and the UN Commission on Crime Prevention and Criminal Justice.

The UNODC has argued, "Several international legal instruments require States Parties to take measures to protect children from abuse and exploitation, as well as to engage in international cooperation in the investigation and prosecution of child abuse and exploitation."[1]

They point out those governments that are parties to the UN Convention on the Rights of the Child have obligations outlined below:

> *Article 19*
> *1. States Parties shall take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person who has the care of the child.*
>
> *2. Such protective measures should, as appropriate, include effective procedures for the establishment of social programmes to provide necessary support for the child and for those who have the care of the child, as well as for other forms of prevention and for identification, reporting, referral, investigation, treatment and follow-up of instances of child maltreatment described heretofore, and, as appropriate, for judicial involvement.*
>
> *Article 34*
> *States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent:*
> *(a) The inducement or coercion of a child to engage in any unlawful sexual activity;*
> *(b) The exploitative use of children in prostitution or other unlawful sexual practices;*
> *(c) The exploitative use of children in pornographic performances and materials.*
>
> *Article 35*
> *States Parties shall take all appropriate national, bilateral and multilateral measures to prevent the abduction of, the sale of or traffic in children for any purpose or in any form.*

[1] UN Office on Drugs and Crime, 'Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children', 2015, 36.

Article 36
States Parties shall protect the child against all other forms of exploitation prejudicial to any aspects of the child's welfare.

The Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography requires governments to:

Article 9
1. States Parties shall adopt or strengthen, implement and disseminate laws, administrative measures, social policies and programmes to prevent the offences referred to in the present Protocol. Particular attention shall be given to protect children who are especially vulnerable to such practices.

Article 10
1. States Parties shall take all necessary steps to strengthen international cooperation by multilateral, regional and bilateral arrangements for the prevention, detection, investigation, prosecution and punishment of those responsible for acts involving the sale of children, child prostitution, child pornography and child sex tourism. States Parties shall also promote international cooperation and coordination between their authorities, national and international non-governmental organisations and international organisations.

The UNODC has also argued that the UN Convention against Transnational Organised Crime requires governments to implement measures to prevent, investigate and prosecute any "serious crime" as defined in Article 2(b) of the Convention.[2] The UNODC states that "serious crime" includes the online abuse or exploitation of children, when the minimum punishment for the specific national crime in question amounts to four years imprisonment or more.[3] They have argued that the Convention requires governments to act on crimes that involve an organised criminal group benefiting from "sexual gratification, such as the receipt or trade of materials by members of child grooming rings, the trading of children by preferential child sex offender rings or cost-sharing among ring members."[4]

The UNODC has argued that there is a need to balance treaty-based human rights. They state that in 2011 the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression identified four forms of expression that are required to be prohibited by government actions under international law: child sexual abuse; direct and public incitement to commit genocide; advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence; and incitement to terrorism.[5]

The UN Commission on Crime Prevention and Criminal Justice passed a resolution on 24 May 2019 that called for governments to "grant law enforcement agencies appropriate powers and to provide tools to identify perpetrators and victims and effectively combat child sexual exploitation and sexual abuse."[6] The resolution also called on Governments:

[2] Ibid., 37.
[3] Ibid., 37.
[4] Ibid., 37.
[5] Ibid., 55.
[6] UN Economic and Social Council, Commission on Crime Prevention and Criminal Justice, 'Countering child sexual exploitation and sexual abuse online', E/CN.15/2019/L.3/Rev.1, 24 May 2019, 3.

> *"…to take legislative or other measures in accordance with domestic law to facilitate the detection by internet service and access providers or other relevant entities, of child sexual exploitation and sexual abuse materials, and to ensure in compliance with domestic law the reporting of such materials to the relevant authorities and their removal by internet services and access providers or other relevant entities, including in conjunction with law enforcement;*
>
> *…to keep an appropriate balance between the development and implementation of privacy protection policies and efforts to identify and report online child sexual abuse materials or online child exploitation offences."*

The Synod believes that, in contrast to UNODC, UNICEF, UNESCO, and the UN Commission on Crime Prevention and Criminal Justice, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has been on his own amongst UN bodies in emphasising the right to privacy and freedom of expression over granting law enforcement agencies effective tools to deal with severe human rights abuses perpetrated or facilitated online.

It is the view of the Synod that the Commonwealth Government would not be honouring its human rights obligations under the treaties it is a party to if it were to give ultimate priority to the right to privacy of those suspected of committing child sexual exploitation and other serious human rights abuses to the point of undermining the ability of law enforcement agencies to be able to effectively prevent such abuses and crimes. The resulting serious harms inflicted on people would be grossly disproportionate to the privacy benefits provided.

4. Trends and changes in relation to the crime of online child exploitation

"Child sexual abuse is a life changing adversity and an injury which research now reveals can manifest a harmful impact upon a child's physical health, immunity, ability to learn, to grow, and mental well-being. Children with pre-existing health problems often have worsening of symptoms when they suffer this and other forms of abuse. Survivors tell us that the memorialisation of child sexual abuse through the production of abusive images and videos and even worse, its distribution, constitutes a most egregious insult to an already severe injury."[7]
Dr Sharon Cooper, Development and Forensic Paediatrician and Adjunct Professor of Paediatrics, University of North Carolina at Chapel Hill School of Medicine

The emergence of the online world has dramatically facilitated the rape, torture and sexual abuse of children across the globe. Child sexual abuse perpetrators can now find their victims online by using advanced technologies and taking advantage of online platforms and services to go undetected. They are also able to set up their own forums and sites to share information and tips with a spirit of camaraderie.[8] They share information about which global locations are most convenient for opportunities to sexually abuse children.[9] The ability to find like-minded people online, which helps to socialise and normalise child abuse, can make it harder for those with a disposition for paedophilia to control their behaviour.[10] It has also resulted in increased production of new child sexual abuse material to share online, as child sexual abuse perpetrators in networks try to please each other with the sharing of such material.[11]

Research and the experience of law enforcement agencies demonstrates that criminals engaged in the rape, torture and sexual abuse of children of all ages and who trade in images, videos or stream such horrific activity are adaptive. 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.

4.1 Prevalence and characteristics of online child exploitation

The children's rights network Terre des Hommes has estimated that there will be roughly 750,000 men worldwide looking for online sex with children at any time of the day.[12]

As of August 2017, the Internet Child Sexual Exploitation Database contained over one million unique images and videos.[13] Only a small fraction of the children captured in this material have

[7] Canadian Centre for Child Protection, 'How we are failing children: Changing the paradigm', 2019, 3.
[8] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 7; and Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 142-143.
[9] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 8.
[10] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 143.
[11] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 10.
[12] 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.
[13] Canadian Centre for Child Protection, 'How we are failing children: Changing the paradigm', 2019, 14.

been identified. Globally, law enforcement agencies have only been able to identify 19,100 of the children depicted in child sexual abuse material online.[14]

The eSafety Office assisted in the facilitation of the takedown of more than 5,000 child sexual abuse items hosted overseas in the 2016-2017 financial year and more than 8,000 such items in the 2017-2018 financial year.[15] The eSafety Commissioner reported that it identified over 13,000 cases of online child sexual abuse material in the 2019-2020 financial year.[16] They requested the removal of 4,000 items of image-based abuse on 248 platforms. The removal was successful in 82% of cases.[17]

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 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.[18] 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.[19] 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.[20] In part, the increase has been driven by greater compliance with reporting suspicious transactions by money service businesses in the Philippines.[21]

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.[22] 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.[23] These 21 suspected offenders spent a median amount of $75 per transaction. The median number of days between transactions was seven.[24] Twelve of the 21 suspected offenders had a prior criminal history.[25] However, only one of these had a previous history of sexual offences against children.[26]

---

[14] US National Center for Missing and Exploited Children, https://www.missingkids.org/footer/media/keyfacts
[15] Lynelle Briggs, 'Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the *Broadcasting Services Act 1992* (Online Content Scheme), October 2018, 11.
[16] ACMA and eSafety Commissioner, 'Annual Reports 2019-20', October 2020, 203.
[17] Ibid., 216.
[18] Simon Benson, 'Agencies link 256 to online child sex', *The Australian*, 19 February 2020, 1.
[19] Republic of the Philippines Anti-Money Laundering Council, 'Online Sexual Exploitation of Children', 2020, 5, 8.
[20] Ibid., 11.
[21] Ibid., 11.
[22] 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.
[23] Ibid., 3-4.
[24] Ibid., 6.
[25] Ibid., 6.
[26] Ibid., 8.

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.[27] There was also an increase in the number of individual images of children being hosted, with 293,818 images being viewed.[28] In 2018, the Internet Watch Foundation removed 105,047 webpages showing sexual abuse and sexual torture of children.[29] Trend data from the UK Internet Watch Foundation has shown the proportion of images of victims of child sexual abuse under the age of 10 has been decreasing, as shown in Table 1.

Table 1. The proportion of images viewed by the Internet Watch Foundation showing victims of child sexual abuse under the age of 10, 2011 -2019.[30]

Year	2011	2012	2013	2015	2016	2017	2018	2019
The proportion of images showing victims of child sexual abuse under the age of 10	74%	81%	81%	69%	53%	55%	40%	46%

In 2016 and 2017, 2% of the images detected by the Internet Watch Foundation involved the sexual abuse of children aged two or under.[31] In 2018, the Internet Watch Foundation reported that it viewed 1,300 images of the sexual abuse of infants and babies.[32]

The proportion of images of child sexual abuse showing sexual activity between adults and children, including rape and sexual torture decreased, as shown in Table 2.

Table 2. The proportion of images viewed by the Internet Watch Foundation showing penetrative sexual activity involving children including rape and sexual torture 2011 – 2019. [33]

[27] Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', 15; and Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', 6, 17.
[28] Internet Watch Foundation, 'IWF Annual Report 2016', 6.
[29] Internet Watch Foundation, 'Record number of images showing children being sexually abused removed by UK internet charity', 23 January 2019.
[30] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', 11; Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', 6; Internet Watch Foundation, 'IWF Annual Report 2016', 9; Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', 6.
[30] Internet Watch Foundation, 'IWF Annual Report 2016', 9; Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', 6; Internet Watch Foundation, 'Record number of images showing children being sexually abused removed by UK internet charity', 23 January 2019; and Internet Watch Foundation, 'The Why. The How. The Who and the Results. The Internet Watch Foundation Annual Report 2019', 2020, 47.
[31] Internet Watch Foundation, 'IWF Annual Report 2016', 9 and Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', 6.
[32] Internet Watch Foundation, 'Record number of images showing children being sexually abused removed by UK internet charity', 23 January 2019.
[33] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', 11; Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', 6; Internet Watch Foundation, 'IWF Annual Report 2016', 9; Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', 16; and Internet Watch Foundation, 'The Why. The How. The Who and the Results. The Internet Watch Foundation Annual Report 2019', 2020, 48.

Year	2011	2012	2013	2014	2015	2016	2017	2018	2019
The proportion of images showing penetrative sexual activity with children	64%	53%	51%	43%	34%	28%	33%	23%	20%

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 3. 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 3. The number of reports of online child sexual abuse material reported to the US National Centre for Missing and Exploited Children 2014-2020.[34]

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.[35] Google provided 449,283 of the reports (2.7%).[36] Only 150,667 reports (0.89%) of online child sexual abuse reported to the US National Center for Missing and Exploited Children came from members of the public.[37]

In 2020, Facebook made 20.3 million (94%) of the reports to the US National Center for Missing and Exploited Children.[38] Google provided 546,704 of the reports (2.5%).[39] The number of reports from the public increased to 303,299 (1.39%).

Since its inception in 1998, the US Cyber Tipline to receive reports of online child sexual abuse has received 82 million reports of such abuse.[40]

The Internet Watch Foundation reported detecting 571 newsgroups that hosted child sexual abuse material in 2017 compared to 455 in 2016.[41]

---

[34] 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.
[35] US National Center for Missing and Exploited Children, '2019 Reports by Electronic Service Providers (ESP)', 2020, 2.
[36] Ibid., 2.
[37] US National Center for Missing and Exploited Children, https://www.missingkids.org/footer/media/keyfacts
[38] US National Centre for Missing and Exploited Children, '2020 Reports by Electronic Service Providers (ESPs)', 2021, 2.
[39] Ibid., 2.
[40] US National Center for Missing and Exploited Children, https://www.missingkids.org/footer/media/keyfacts; https://www.missingkids.org/theissues/csam
[41] Internet Watch Foundation, 'IWF Annual Report 2016', p. 8; and Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', 15.

The Internet Watch Foundation reported that in 2016, offenders distributing child sexual abuse imagery commonly use image hosts to host the images that appear on their dedicated websites. These websites can often display many thousands of abusive images.[42]

In terms of online media hosting child sexual abuse images, in 2016 the Internet Watch Foundation reported they had detected such material on 41,364 image hosts, 6,223 cyberlockers, 2,776 banner sites, 1,681 image boards, 826 blog sites, 803 online forums, 727 web archives, 643 social networking sites and 634 images stores.[43]

In 2019, the Internet Watch Foundation reported that child sexual abuse material was hosted on the following platforms:[44]

- Image host (84%);
- Cyberlocker (6%);
- Banner site (2%);
- Website (2%);
- Forum (2%);
- Video channel (1%);
- Image board (less than 1%);
- Search provider (less than 1%);
- Social networking (less than 1%); and
- Web archive (less than 1%).

In 2019, the Internet Watch Foundation reported that 5% of the URLs containing child sexual abuse material were commercial sites.[45] Commercial sites are run as for-profit businesses.

The Financial Times reported that videos and images of children being sexually abused were being openly shared on Facebook's WhatsApp on a vast scale.[46] Israeli researchers warned WhatsApp that it was easy to find and join dozens of chat groups where people were sharing images and videos of children being sexually abused. In one case, one of these groups had 256 members.

4.2 The voices and experiences of survivors

The following are direct quotes from survivors of child sexual abuse who had images, videos or live streaming of their abuse placed online. The survivors responded to a global survey conducted by the Canadian Centre for Child Protection in 2016. The survivors consented to their voices being heard publicly, so others would have a better understanding of what they have been through and the impact it has had on their lives. These voices should help shape the response to the issue of regulation of the online world.

---

[42] Internet Watch Foundation, 'IWF Annual Report 2016', 11.
[43] Ibid., 11.
[44] Internet Watch Foundation, 'The Why. The How. The Who and the Results. The Internet Watch Foundation Annual Report 2019', 2020, 51.
[45] Ibid., 51.
[46] Leila Abboud, Hannah Kuchler and Mehul Srivastava, 'WhatsApp fails to curb sharing of child sex abuse videos', *The Financial Times,* 20 December 2018, https://www.ft.com/content/bff119b8-0424-11e9-99df-6183d3002ee1

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

Quotes from survivors of online child sexual abuse.

Warning: Some of these quotes may cause distress.

"I was systematically trained down in advance regarding crying and screaming during the abuse by being pushed underwater until losing consciousness when I cried or screamed. Vomiting was forbidden, too, which I was supposed to learn to stop doing by having to eat my vomit again, which generally made me throw up again and have to eat it again. That often went on so long until the circulatory system stopped playing along. I had to pretend I liked being raped. For other acts, in contrast, it was important to plead and beg the perpetrator to stop. Sometimes, I and other children were forced to commit violent acts on other children. I'm not sure whether all of these videos survived."[47]

"After the abuse had continued for some time, I tried to wrestle myself away from him. But he was strong as a bear (in my perception at least). So I tried to physically resist, he put me in a sort of hold and then went ahead with abusing me. He didn't photograph that, though, because he had his hands full with me. But here again, the message was clear: I'd never be able to win against him."[48]

"He threatened to tell my family everything… He threatened to wreck my life… I'd no longer have any ground under my feet to exist… I'd be better off committing suicide myself before he got hold of me because that would be gruesome. I was to never tell about it ever."[49]

"Perpetrators spoke a lot over my head. How many films they already had; what they could earn from them etc. It was never discussed with me, but I picked up a lot."[50]

"I was threatened that the prosecution authorities would receive the videos in the event of a complaint so that they could see that I had wanted everything was I was the real perpetrator. On another occasion, I was told the material would be distributed and then the whole world would know how disgusting and dirty I am, no matter where I go."[51]

"He made me hold signs with messages on them for other paedophiles so that he could get what he wanted from them by making custom videos."[52]

"Look at it like this. The hands-on was horrible. But at the very least, it is over and done with. The constant sharing of the abuse will never end; therefore, the remainder of its existence will never end… If you ask me, a crime that never ends is worse than one that is over; no matter how much more serious it may appear. That this is something inescapable. That there will never be total absolution."[53]

[47] Canadian Centre for Child Protection, 'Survivors' Survey. Full Report 2017', 2017, 53.
[48] Ibid., 58.
[49] Ibid., 61.
[50] Ibid., 65.
[51] Ibid., 65.
[52] Ibid., 69.
[53] Ibid., 149.

"The experiences are over. I can get a certain measure of control over those experiences. With regards to the imagery, I'm powerless. I can't get any control. The images are out there."[54]

"The abuse suffered influences inside, although symptoms also are evident on the outside. The existence and distribution of the material make me feel ashamed, and I live under constant fear that other people could recognise me and know about it. It triggers the feeling that one can never escape from these experiences."[55]

"When talking to people about child abuse, and I mention that I was in pictures/ child porn, I'm not treated the same afterwards. People avoid me when they know that. It's like the fact that I was victimised in my childhood by sexual photography makes me feel victimised again as an adult. People understand hands-on but not what you call child sexual abuse imagery. There is an extra stigma if one was victimised in that way. I'm made to feel ashamed every time I mention it because people, even friends, can't look at me, and change the subject if I mention it. But that doesn't happen if I mention hands-on sexual abuse."[56]

"The imagery abuse impacts me differently than the hands-on abuse because now, THOUSANDS of people are taking advantage of me. Their argument is that they aren't physically abusing me, so there's no "harm" being done. They are insane for thinking this way. Those are sexual images that were taken of me as a CHILD. These people are degrading me every second they look at those photos. I did NOT get a choice in taking those photos. It was ABUSE, and when they are looking at them, and doing whatever it is that they are doing, they are abusing me all over again. The abuse will NEVER end for me. I am never safe. I don't get to live a normal life where I can take pictures at the beach and feel comfortable. I feel like I am constantly naked, like, I will never have a clear mind because I know somewhere someone is looking at my photos right now. It could be someone from another country or maybe even someone I work with. I am terrified for my life. I constantly have thoughts of someone finding out who I am and trying to hurt me."[57]

"My experiences impact (and have impacted) virtually every possible area of my life. My relationship with my body is always disturbed, and I live with enormous hatred towards myself. I'm constantly absorbed with death, and it's a very tough struggle not to give in to suicidal thoughts or destructive behaviours (such as cutting). For fifteen years, right from childhood, I've had an eating disorder. For it, I took part in a five-day intensive (inpatient) course of nutrition therapy several years ago. I have difficulty with men, setting limits, sexuality, intimacy, trust, and I often suffer anxiety and nightmares. I feel extremely ashamed of myself and of my experiences. I'm constantly afraid that people are angry at me and that the rest of the world hates me. I suffer from intrusive flashbacks, in which I relive my traumatic and other experiences. Due to my experiences, I have no more contact with my family. I often feel terribly lonely, isolated, depressed and a burden."[58]

[54] Ibid., 149.
[55] Ibid., 152.
[56] Ibid., 152.
[57] Ibid., 153.
[58] Ibid., 156-157.

Of the 150 survivors who responded to the Canadian Centre for Child Protection in 2016, 96 reported that had been subjected to threats related to the sexual abuse they had been subjected to. Of these:[59]

- 67% of the respondents were threatened with physical harm. Of those, 44% were told they would be murdered if they did not comply;
- 24% of respondents were threatened with physical harm to a family member. Of those, 61% were told the family member or members would be murdered if they did not comply;
- 19% of the respondents were threatened with physical harm to other people or animals in their life. Of those, 50% were told that those people or animals would be killed if they did not comply.

Some survivors reported they had been tortured with electric shocks, being held underwater or choked to force their compliance.[60]

4.3 The socialisation of offenders

We all are subject to socialisation. Socialisation is the process where we acquire our attitudes, values, beliefs and behavioural patterns in conformity with the demands of the society or group to which we belong.[61] Successful socialisation of a person is marked by acceptance of the society or group the person is part of. Anyone who has joined a hobby or interest group or a church congregation knows that each such group has its own culture, its own accepted norms in the group. You will often modify your behaviour to fit in. This has a downside, as behaviours that were initially troubling to you, or made you feel uncomfortable, may start to feel normal over time.[62]

In the online world, people with very disturbing or harmful behaviours are often able to forms groups that amplify the problematic behaviour. They are free from being challenged by the wider society.

You can easily stumble upon a behaviour online and immerse yourself in new worlds and new communities, becoming cyber-socialised to accept activities that would have been unacceptable just a decade ago. The previously unimaginable is now just at your fingertips – just waiting to be searched.[63] People therefore can be drawn into networks of child sex abusers and become socialised into such networks.

One of the powers of the cyber environment is its ability to deceive and delude. It attracts vulnerable individuals into strange communities where their desire for acceptance becomes an obsession.[64]

Networks of child sexual abuse perpetrators have developed online handbooks and manuals to assist each other. These handbooks are highly detailed and instructive in content.[65] They will

[59] Ibid., 56.
[60] Ibid., 57.
[61] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 37.
[62] Ibid., 38.
[63] Ibid., 45.
[64] Ibid., 153.
[65] UK Ministry of Justice, 'Serious Crime Act 2015. Fact sheet: Offence of possession of paedophile manuals', March 2015,

contain advice on how to entrap or groom a child, where to find a child victim, how to offend and escape capture.[66] For example, in November 2018 a man was imprisoned in the UK who had in his possession five child sexual abuse manuals, including a Harry Potter-inspired child sexual abuse manual.[67] He had a three-part manual that contained guidance on how to abuse children aged between five and eight. These include advice on how to sexually abuse a child 'safely', as well as how to win a child's obedience and cooperation. The 24-page manual, which used references taken from the Harry Potter series of books, contained technical guidance on how not to be caught by the police. In the US in 2018, a man was imprisoned for child sexual abuse offences who had in his possession a downloaded copy of the 576 page 'The Pedophile's Handbook'.[68] The handbook included chapters such as "Finding Children" and "Hunting Season". One chapter offered help to readers to "learn the basics about how to find yourself children through various methods, and how to befriend them."[69] Another offered to help readers learn "how to stay secure as an active paedophile and how to handle civilians and police, even prisons if things should go really wrong."[70]

The networks of perpetrators also target survivors for further harassment and abuse. For example, perpetrators will post online information about survivor's current whereabouts and other identifying information. Such information may include the school or university they attend, the name of the sports team the survivor is on, a survivor's community involvement and images of the survivor's friends. There have been some extreme instances where perpetrators seek images of survivors, now as adults, with their families and comment on their desire to offend against the survivor's children.[71]

There has been a shift in the demographic of people accessing child sexual abuse material, with an increase in younger people accessing such content.[72]

4.4 Sexual extortion of children online

As more children have access to the Internet and social media platforms, there is a reported increase in the number of cases of sexual extortion involving children.[73] A US National Centre for Missing and Exploited Children study found that in 78% of reported sexual extortion cases, the victim was female and aged between 8 and 17.[74]

---

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415982/Fact_sheet_-_Paedophile_manuals_-_Act.pdf
[66] Ibid.
[67] UK Crown Prosecution Service, 'Man jailed for possessing paedophile manuals', 5 November 2018, https://www.cps.gov.uk/london-north/news/man-jailed-possessing-paedophile-manuals
[68] 'Man With 'Pedophile's Handbook' Gets 37 Years For Making, Possessing Child Porn', 2 May 2018, https://www.nbcchicago.com/news/local/man-with-pedophiles-handbook-gets-37-years-for-making-possessing-child-porn/48474/
[69] Ibid.
[70] Ibid.
[71] Canadian Centre for Child Protection, 'How we are failing children: Changing the paradigm', 2019, 20.
[72] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 143.
[73] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 1.
[73] Ibid., 13.
[74] Ibid., 14.

Recent investigations have uncovered the existence of organised sexual extortion groups. These groups operate across borders and use call centre-like operations in order to communicate with hundreds of potential victims at once.[75]

In the online space, teenagers often exhibit a lack of concern for privacy. Paradoxically, usually in the real world, many teenagers are self-conscious and seek privacy. Online even teenagers who are well versed in the dangers and have read stories of identity theft, sexual extortion, cyberbullying, and cybercrimes continue to share personal information as though there is no risk.[76] Such teenagers become more vulnerable to the risk of being targeted for sexual extortion. Professionals working to address online child sexual abuse reported an increase in risk taking behaviour online by minors during the COVID-19 pandemic.[77]

The negative psychological impacts of sexual extortion include feelings of low self-esteem, withdrawal, worthlessness, anger and guilt. In some cases, victims have engaged in self-harm or killed themselves.[78]

[75] Ibid., 14.
[76] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 196.
[77] Michael Salter and 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, 5.
[78] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 14.

5. The efficacy and gaps in legislative tools and tactics of law enforcement

5.1 The challenge of general deterrence in the online world

It needs to be recognised that the majority of people will not be inclined to commit crimes that are contrary to the cultural norms of their society, regardless of the risk of being caught or the severity of the penalty. However, if an environment makes it easy to commit a crime and get away with it, then more people will be tempted to commit the crime.

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. For example, most people would regard going to prison for five years is something they would want to avoid. Increasing the penalty for a particular crime from five years in prison to 10 years in prison will only have a small impact on the number of people who would be willing to commit the crime. What will have a much greater impact is the risk of being caught and the risk of the penalty being applied if the person gets caught.

Review of criminological literature on what works to deter crime finds that there is substantial evidence that the increased visibility of law enforcement personnel and allocating them in ways that materially heighten the perceived risk of apprehension can deter crimes.[79] The literature on crime finds that perceived certainty of punishment is associated with reduced intended offending.[80] The conclusion is that certainty of apprehension and not the severity of the legal consequences ensuing from apprehension is the more effective general deterrent.[81]

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 higher levels of serious criminal behaviour mean that police can deal with a shrinking portion of the online criminal behaviour, which in turn increases the level of people engaged in severe criminal behaviour. It becomes a vicious circle.

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

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

[79] Daniel S Nagin, 'Deterrence in the Twenty-First Century', *Crime and Justice* Vol. 42, No. 1, (August 2013), 201.
[80] Ibid., 201.
[81] Ibid., 202.

adequately handle the volumes of cases of online child sexual abuse they know of.[82] 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 or reduce its profitability. These tools provide greater deterrence for people who would otherwise succumb to the temptation to engage in criminal activity online.

An example of a mass detection tool is Project Arachnid. Project Arachnid is a technological tool designed to reduce the availability of child sexual abuse images online.[83] 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 have sent more than 3.6 million notices for removal of child sexual abuse material to online providers.[84] 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.[85] 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.[86]

The UN Office on Drugs and Crime has recommended that governments need to draft their laws to prevent serious online harm as being flexible and "technology-neutral" to keep up with technological innovation without needing constant reform.[87] They have also stated that laws and international cooperation mechanisms must also address the need for timely access to information across national boundaries.[88]

Requirements that increase the workload for law enforcement agencies reduce the number of cases of serious criminal activity that can be investigated and prevented. Thus, increasing requirements on law enforcement come at the cost of an increased number of victims of serious criminal activity, including a greater number of children raped, tortured and abused. For example, in Canada, police are now required to obtain a judicial authorisation signed by a judge to have an Internet Service Provider tell the police the identity of people using their service. The requirement has significantly reduced the number of cases of online child sexual abuse that

[82] 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.
[83] Canadian Centre for Child Protection, 'Australia's hotline joins global project combating online child abuse', Media release, 5 June 2019.
[84] Ibid.
[85] https://projectarachnid.ca/en/
[86] Ibid.
[87] UN Office on Drugs and Crime, 'Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children', 2015, 55.
[88] Ibid., 55-56.

Canadian police can investigate.[89] In Australia, police can obtain such information with a simple request. They only need a court-issued warrant if they wish to access the content of what a person is communicating or accessing.

The increasing use of encryption is limiting the ability of police to investigate online child sexual abuse.[90]

Effective law enforcement online also requires that law enforcement agencies have access to tools and data that allow them to identify others involved in a network of criminal activity when they find an individual in the network.[91] Access to the data that shows interactions between people also allows police to identify those facilitating severe criminal activities, such as businesses providing encrypted communication.[92] Such data can also help police locate victims[93], to rescue them from further harm.

5.2 Destruction of evidence by ICT corporations

The 2018 documentary, 'The Cleaners', has exposed how technology companies 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.

It is not clear that when a technology corporation sub-contracts content managers that results in the destruction of evidence of child sexual abuse in another jurisdiction that involves an Australian victim or perpetrator they can be held to account under current Australian laws. As an example of such a scenario:

- An Australian citizen living in the UK engages in online sexual abuse of a child located in Australia;
- The technology corporation states that record of the abuse is located on a server in Ireland; and
- A subcontracted content manager in the Philippines is required to destroy the evidence of the abuse that occurred.

Given the complexity of where the destruction of the evidence occurred, the Committee should explore the ability of Australian law to hold the corporation to account for the destruction of the evidence, including the individuals in the corporation that set up the system that allowed the evidence to be destroyed.

Recommendation: Australian law makes it an unambiguous offence for a technology provider not to preserve and report evidence of child exploitation on their platform to law

[89] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 5.
[90] Ibid., 6.
[91] Australian Criminal Intelligence Commission, 'Submission to the Parliamentary Joint Committee on Intelligence and Security Review of Mandatory Data Retention', July 2019, 3.
[92] Ibid., 3.
[93] Ibid., 4.

enforcement agencies where an Australian child or offender is involved or where the provider is located in Australia.

5.3 The problem of obtaining online evidence across borders

The current online world allows technology corporations to arbitrarily decide where the server holding relevant evidence of serious human rights abuses and criminal activity is hosted, regardless of where the perpetrator is located, or the victim is located. The result has been an increasing number of Mutual Legal Assistance requests from law enforcement agencies across the globe to obtain information that the technology corporation has decided in located in another jurisdiction. A Mutual Legal Assistance request often takes the best part of a year to get a response. It is our understanding that on average, it takes Australian law enforcement agencies 10 to 12 months to receive even basic communications data after filing a Mutual Legal Assistance request. In some cases, obtaining communications data from a Mutual Legal Assistance request can take up to 18 months. In April 2018, the EU Commission reported that the average length of time taken to obtain a response to a Mutual Legal Assistance request within the EU was ten months.[94] However, the Council of Europe Cybercrime Convention Committee found in 2014 that the average response time to a Mutual Legal Assistance request was six months to two years.[95] The Committee found because of the long delays posed by Mutual Legal Assistance requests:[96]

> *Many requests and thus, investigations are abandoned. This adversely affects the positive obligation of governments to protect society and individuals against cybercrime and other crime involving electronic evidence.*

Most requests were for simple subscriber data, to know who a suspect is in the first place. The Committee reported that not being able to identify the suspected offender because of not having the subscriber data prevented criminal investigations.[97] Gail Kent from the Centre for Internet and Society ay Stanford Law School stated in 2015 that in the UK requests for communications data through a Mutual Legal Assistance request would take up to 13 months.[98] The EU Commission has assessed that, "The current procedures for cooperation between judicial authorities to obtain e-evidence in cross-border situations are too slow compared to the speed at which electronic data can be changed or deleted."[99] The victims and survivors of sexual abuse and other crimes deserve better.

Even when the information is eventually provided, the law enforcement agency or prosecutor may find it is incomplete, or it may open up a new lead, that requires yet another Mutual Legal Assistance request. The Synod has spoken with prosecutors who say that if evidence for a trial needs to be obtained by a Mutual Legal Assistance request, then they build their case on the assumption the information will not be available in time to be used. The result is that people who

[94] European Commission, 'Frequently Asked Questions: New EU rules to obtain electronic evidence', Brussels, 17 April 2018, 1.
[95] Council of Europe, Cybercrime Convention Committee, 'Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY', 16 September 2016, 11.
[96] Council of Europe, Cybercrime Convention Committee, 'Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY', 16 September 2016, 11.
[97] Council of Europe, Cybercrime Convention Committee, 'Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY', 16 September 2016, 11.
[98] Gail Kent, 'The Mutual Legal Assistance problem explained', The Centre for Internet and Society, Stanford Law School, 23 February 2015,
[99] European Commission, 'Frequently Asked Questions: New EU rules to obtain electronic evidence', Brussels, 17 April 2018, 1.

have committed online child exploitation or other serious human rights abuses escape justice because the online world created by ICT corporations makes it hard to obtain the evidence.

Recommendation: The Parliament pass the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* after the Government responds to the recommendations of the Parliamentary Joint Committee on Intelligence and Security.

5.4 Opposition to effective law enforcement tools to prevent online child sexual abuse

Organisations that campaign against effective law enforcement tools to prevent online child sexual abuse 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:[100]

> *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.*

Opponents of effective police powers to address online child sexual abuse and other serious harms often claim technical expertise to bolster their opposition. However, such claims need to be tested against research and actual real-world experience. For example, many of these Australian opponents to online regulation made claims that have proven to be untrue about the consequences of Internet Service Providers (ISPs) being required to disrupt ready access to online child abuse material. Under the previous Labor Government, many of these individuals and groups claimed that requiring ISPs to disrupt ready access to child abuse material would have disastrous impacts on the Internet and the speed of the Internet would be greatly impacted.[101] The vast majority of Australian internet traffic is now disrupted from accessing child abuse material on the Interpol 'worst of the worst' list of sites displaying child sexual abuse material. The Australian Federal Police having issued notices to ISPs under section 313 of the Telecommunications Act achieved this. All of the claimed negative impacts on the Internet in Australia because of this access disruption were wrong.

[100] Gail Kent, 'The Mutual Legal Assistance problem explained', The Centre for Internet and Society, Stanford Law School, 23 February 2015,
[101] See for example https://www.efa.org.au/2013/09/06/opt-out-opt-in-the-internet-filter-hokey-pokey/; K Dearne, 'Critics slam Canberra net block plan', *The Australian*, 25 September 2007, 31; https://www.dynamicbusiness.com.au/news/iinet-senator-conroy-liar-filter-1611.html/comment-page-1?page-video419048=6

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

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.[102] 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.[103]

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).[104] 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 assists child sex offenders from evading detection by law enforcement agencies.[105] Those engaged in child sexual abuse online teach each other how to become anonymous online.[106] They are more commonly educating each other on using private chats, Internet voice and video chat software, forums and anonymisation software.[107] The feeling of impunity, because of those carrying out the abuse being able to conceal their identity, has enabled them to diversify their activities.[108]

Online concealment of people engaged in child sexual abuse has facilitated much larger participation in such horrific activities. Hidden online child sexual abuse services commonly contain hundreds or even thousands of links to child sexual abuse imagery hosted on image hosts and cyberlockers on the open web.[109] Child sexual abuse sites on the darknet are particularly being used by offenders to host and distribute sexual abuse material involving infants and toddlers.[110] One such site had over 18,000 registered members who regularly met online to discuss their preference for the sexual abuse of children in this age group.[111] A forum dedicated to discussing the abuse of children exceeded 23 million visits.[112] On another darknet site, each user uploaded one three-minute video or two images each month of child sexual abuse as membership payment.[113]

Child sexual abuse perpetrators operate in networks online to assist each other.[114] 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.[115]

Recommendation: Require technology providers 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 identity suspected

[102] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 14.
[103] Ibid., 14.

people engaged in online child sexual abuse. It would also act as a general deterrent reducing the perception by offenders they will not be identified for their online activities.

6.2 The threat of end-to-end encryption to preventing online child sexual abuse

Facebook plans to implement end-to-end encryption on all its message services. In 2018, Facebook reported 16.8 million suspected posts and messages related to child sexual abuse on their platforms.[116] In the UK alone, these reports resulted in 3,000 children being safeguarded from further child sexual abuse and arrest of 2,500 suspected perpetrators.[117] 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.[118]

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.[119] These threats of changes in online technology corporations' behaviour increase the need for law enforcement to be given effective tools to respond.

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.[120] 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

---

[104] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 5, 15.
[105] 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.
[106] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 15.
[107] Ibid., 16.
[108] Ibid., 5.
[109] Internet Watch Foundation, 'IWF Annual Report 2016', 13 and Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', 20.
[110] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 16.
[111] Ibid., 16.
[112] Ibid., 16.
[113] Ibid., 16.
[114] 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.
[115] Ibid., 15.
[116] 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.
[117] Ibid.
[118] Ibid.
[119] 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
[120] Virtual Global Taskforce position on End-to-End Encryption

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 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.[121] However, it is concerning that Apple will allow users to appeal to Apple against their assessment.[122] 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.

6.2 Concealed child sexual abuse material

The Internet Watch Foundation also reported that in 2016, 2017 and 2019 criminals increasingly used masking techniques to hide child sexual abuse images and videos on the Internet. The criminals leave clues to perpetrators so they can find the conceal child sexual abuse material. Since 2011, the Internet Watch Foundation has been monitoring commercial child sexual abuse websites that only display child sexual abuse imagery when accessed by a "digital pathway" of links from other websites. When the pathway is not followed, or the site is accessed directly through a browser, legal content is displayed. This means it is more challenging to find and investigate illegal imagery. They saw a 112% increase in this technique in 2016 over 2015, with 1,572 sites using this technique in 2016.[123] This increased again in 2017, with 2,909 websites using this method to hide child sexual abuse material.[124] In 2019, they reported they had detected 288 providers of child sexual abuse material that were using hidden services.[125]

[121] 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.
[122] Reed Albergotti, ‘Apple to scan phones for child pornography, sexual messages to minors’, *The Australian Financial Review,* 7 August 2021.
[123] Internet Watch Foundation, ‘IWF Annual Report 2016’, 5, 17.
[124] Internet Watch Foundation ‘Internet Watch Foundation Annual Report 2017’, 24.
[125] Internet Watch Foundation, ‘The Why. The How. The Who and the Results. The Internet Watch Foundation Annual Report 2019’, 2020, 54.

The number of newly identified hidden services (on the 'dark web') detected by the Internet Watch Foundation declined from 79 in 2015 to 41 in 2016 and then increased to 44 in 2017. They postulated that the result could be due to increased awareness by law enforcement internationally about hidden services distributing child sexual abuse imagery.[126]

[126] Internet Watch Foundation, 'IWF Annual Report 2016', 13 and Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', 20.

7. Role of technology providers in assisting law enforcement agencies to combat child exploitation

"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."[127]
Professor Hany Farid, Electrical Engineering & Computer Sciences and the School of Information, University of California

"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."[128]
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"."[129]
Tim Cook, CEO, Apple

7.1 Co-operation and resistance in addressing online child sexual abuse by ICT corporations

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.[130]

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

[127] Canadian Centre for Child Protection, 'How we are failing children: Changing the paradigm', 2019, 3.
[128] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 307.
[129] 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
[130] '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.

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.[131]

US law has assisted US technology corporations not taking responsibility for what is posted on their platforms. The US *Communications Decency Act of 1996* protects technology 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". [132]

The Synod takes the view that when encountering evidence of serious criminal activity, the people running any business would report the evidence of the illegal activity and absorb the cost of doing so. For example, if a rental car business found evidence of bloodstains in one of their vehicles suggesting it had been used in a violent crime, the Synod would expect that the people running the business would report the evidence and preserve it. They would not clean the car and destroy the evidence. If a train company recorded the rape of a child on their service through CCTV, then the Synod would expect that the people running the train business would voluntarily hand over the footage and assist in identifying the rapist to police. The Synod would not expect the train business to seek to uphold the privacy rights of the rapist and hinder the police investigation by wiping the CCTV footage. Unfortunately, the people running multinational technology businesses often appear to fail to live up to this standard, even resisting assisting police when court orders have been issued.

The need for social media and online technology corporations being required to assist law enforcement by force of law is being increasingly recognised globally. For example, the International Centre for Missing and Exploited Children found in 2016 79 governments out of 196 had laws requiring ISPs to retain digital user data to ensure access to data to prosecute child sexual abuse offences.[133]

The key concerns we have with the technology corporations are:

- The lack of inherent safeguards in the products they have created and promote;
- Destruction of evidence of child sexual abuse and other human rights violations without reporting it to law enforcement agencies;
- Claiming that data is not located where the user of their service is, which forces police to have to seek warrants from overseas courts through Mutual Legal Assistance requests, which can take over a year to be resolved;
- Not preserving evidence of child sexual abuse and other human rights violations by allowing users to destroy evidence they have previously posted;
- Obstructing reasonable requests from police investigating child sexual abuse and other human rights violations through the use of court processes in cases where it is clear there are serious human rights violations occurring;
- Not responding quickly enough in removing posts of child sexual abuse or where people are organising human rights abuses; and
- Tipping off human rights abusers, they are under investigation when law enforcement presents a warrant for information about the person unless forbidden from doing so by a court.

[131] Ibid.
[132] Harcher, P., 'Taming big tech's titans', *The Age*, 25 February 2020, 20.
[133] International Centre for Missing and Exploited Children, 'Child Pornography: Model Legislation and Global Review', 8th Edition, 2016, vi.

There are online technology corporations that have an ideological position that the privacy of their clients is paramount. The position leads them to be reckless in designing services that frustrate efforts of police to stop child sexual abuse, terrorism and other dangerous criminal activity.

Other online technology corporations and their management argue they will only assist police to the extent that they are forced to do so by the law. For example, Simon Hackett, the managing director of Internode in 2011, appeared to publicly state that his company would only assist police in combating severe criminal activity to the extent that the law requires them to do so:[134]

> *I can't figure out why people keep thinking ISPs have any interest in forcing their customers to do things against their will, without the ISP being legally required to do so. What is it with that? You don't think we have better things to do with our time and money than to spend millions of dollars imposing transparent packet interception equipment just for kicks?*

Further:[135]

> *We hope that the government won't repeat its previous activity in this realm, of framing ISPs who don't act ahead of, and in the absence of the protection of, some new or existing law as being supporters of the 'bad guys'. We are, of course, not 'supporters of the bad guys'. But we're also not disposed to take actions to impact our customers' Internet services that are not (yet) the subject of any form of legal direction to do so.*

Facebook's policy on retaining evidence of criminal activity on its platform seems reasonable:[136]

> *Information we receive about you (including financial transaction data related to purchases made with Facebook) can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for term breaches for at least a year to prevent repeat abuse or other term breaches.*

However, despite being part of the same multinational corporation, WhatsApp does not make clear how long they will preserve data related to the serious harm of others for criminal investigation for.[137]

By further contrast, Google makes it less clear they will preserve and report actionable child sexual abuse material in all cases:[138]

> *Do not upload or share content that exploits or abuses children. This includes all child sexual abuse imagery (even cartoon images) and all content that presents children in a sexual manner. We will remove such content and take appropriate action, which may include disabling accounts and reporting to the National Center for Missing & Exploited Children (NCMEC) and law enforcement.*

We were unable to identify any part of Google's policies that state how long records of removed content that involve criminal activity would be retained for.

---

[134] https://delimiter.com.au/2011/12/28/post-iinet-internode-maintains-cautious-filter-stance/
[135] https://delimiter.com.au/2011/07/05/well-filter-when-the-law-makes-us-internode/
[136] https://www.facebook.com/about/privacy
[137] https://www.whatsapp.com/legal/#privacy-policy-law-and-protection
[138] https://www.google.com/+/policy/content.html

Multinational ICT corporations have also acted to frustrate the efforts of law enforcement. For example, Brian Lee Davis in the US confessed to owning hundreds of digital photos and videos that showed young children being raped. In July 2017, he was sentenced to a decade in a US state prison. Police sought to pursue the entire child sexual abuse network he had been part of. Police investigators were unable to access emails that could have helped them identify victimized children and track down the offenders Mr Davis admitted to contacting. Although Google tipped off police about the child abuse files that had crossed its network, the corporation refused to give them access to his Gmail account, even though police had a search warrant.[139]

Google's argument was reported to be that the data was "out of jurisdiction." The corporation argued some of the data in that Gmail account were stored on Google servers outside the United States and, since a court ruling in 2016, technology companies were not required to turn over that information.

This highlights the problem where technology corporations can frustrate police investigations by choosing where they say the online data is physically located. Such a choice can be arbitrary, at the total discretion of the technology corporation.

The 2016 US court ruling flowed from a case in 2013 where Microsoft refused to help federal agents in an investigation of drug traffickers, denying them access to emails on computer servers in Dublin. Microsoft's lawyers argued that the 1986 US *Stored Communications Act* did not give police the right to seize information stored in another country without that foreign government's approval.

The company eventually won before the federal appellate court in New York on 14 July 2016. The ruling said the *Stored Communications Act* does not give American judges "extraterritorial" powers, and that therefore they cannot grant search warrants that reach outside the United States. A US judge could not demand that a company give up a video held on a European machine, for instance, even if it documented a crime committed by one American against another on American soil.[140]

Following the legal decision, major technology corporations such as Microsoft and Yahoo defied judges' orders in criminal investigations, refusing to turn over potentially crucial digital evidence of crimes. Their actions impeded hundreds of criminal investigations, according to public testimony to Congress and interviews with law enforcement officials by CNN.[141] These cases include human trafficking, drug smuggling, and fraud.

In the case of the murder of Lucy McHugh, aged 13, Facebook refused to allow UK police access to Lucy's account to determine what was communicated between her and her murderer Stephen Nicholson, aged 25. Facebook's resistance was despite pleas from Lucy's mother that Facebook co-operate with the police.[142] Lucy from Southampton was found in woodland at Southampton Sports Centre after being stabbed to death on 25 July 2018. Stephen Nicholson, a

[139] https://money.cnn.com/2017/10/19/technology/criminal-investigations-microsoft-ireland-invs/index.html
[140] https://money.cnn.com/2017/10/19/technology/criminal-investigations-microsoft-ireland-invs/index.html
[141] https://money.cnn.com/2017/10/19/technology/criminal-investigations-microsoft-ireland-invs/index.html
[142] Shehab Khan, 'Lucy McHugh: Murdered schoolgirl's mother urges Facebook to give suspects' password to police', *The Independent,* 4 September 2018, https://www.independent.co.uk/news/uk/crime/lucy-mchugh-mother-facebook-password-urges-police-stacey-white-stephen-nicholson-a8521761.html

family friend who was staying in Lucy's home until shortly before her death. He was questioned on suspicion of murder and sexual activity with a child but twice refused to give detectives his Facebook password.[143] Mr Nicholson was sentenced to 14 months imprisonment over his refusal to hand over the password to his account. Failing to cooperate with police is an offence under the UK *Regulation of Investigatory Powers Act*. Facebook argued that it would only grant UK police access to Facebook accounts if compelled to do so by a US court.[144] Facebook insisted on a Mutual Legal Assistance Treaty request, which would have taken many months to resolve.[145] We were unable to find any reports if Facebook granted police access to Ms McHugh's account. If not, then this raises serious concerns that the corporation treats user data as its own. Given the clear desire of the parent of the murdered child for Facebook to co-operate with police, Facebook should have granted police access to Ms McHugh's account. The case highlights the need for laws that allow law enforcement agencies to work quickly in the interests of justice and avoid overly long and complicated legal processes. Facebook received sharp public criticism for its accessing user data to target advertising at them while claiming to protect user privacy in the case of a murdered child.[146]

Police were finally able to access Stephen Nicholson's Facebook account just before his trial, but by that time of the evidence of his messages to Lucy had been destroyed.[147] The media report does not indicate who destroyed the evidence.

Stephen Nicholson was convicted of the rape and murder of Lucy McHugh in July 2019.[148] He was convicted on three counts of rape. He was also convicted of sexual activity with a 14-year-old girl in 2012, who he had taken to the same woodland where he later murdered Lucy.[149] Mr Nicholson told police that Lucy had sent him a message the night before he murdered her, saying she was pregnant.[150] After luring her to woodland, Mr Nicholson stabbed her 11 times in the neck in a pre-meditated attack. Lucy was not pregnant.[151]

However, technology corporations do often comply with warrants and subpoenas. Facebook received 32,716 requests for information from US law enforcement agencies between January 2017 and June 2017, covering 52,280 user accounts and included 19,393 search warrants and 7,632 subpoenas.[152] In the same period, Google received 16,823 requests regarding 33,709

[143] Ibid.
[144] Alex Hern, 'Why won't Facebook give access to Lucy McHugh murder suspect's account', *The Guardian,* 6 September 2018, https://www.theguardian.com/uk-news/2018/sep/05/why-wont-facebook-provide-access-lucy-mchugh-suspect-account
[145] Ibid.
[146] Mick Hume, 'Facebook's two-faced bosses show disregard for murdered Lucy McHugh's case as they protect his suspected killer', *The Sun,* 6 September 2018, https://www.thesun.co.uk/news/7188577/mick-hume-facebook-lucy-mchugh/
[147] 'Lucy McHugh: Stephen Nicholson guilty of murder and rape', BBC News, 18 July 2019, https://www.bbc.com/news/uk-england-hampshire-48968498
[148] Ibid.
[149] Ibid.
[150] Ibid.
[151] Ibid.
[152] '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.

accounts, and Twitter received 2,111 requests regarding 4,594 accounts.[153] Each corporation produced at least some information for approximately 80% of requests.[154]

Some ICT corporations also use proactive prevention methods to stop known child sexual abuse material from being uploaded onto their platforms. They can carry out doing so without seeing the content of user's communication in a similar way to how anti-virus software is deployed.[155]

There is a need to ensure that where Australian laws require technology corporations to assist in the investigation and prosecution of child sexual abuse offenders, individuals in the technology corporation can be prosecuted for refusing to co-operate. The ability to prosecute these individuals should be targeted at those who ultimately are responsible for the decision not to co-operate. 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:

> *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.*[156]

Recommendation: Existing legislation should be reviewed and amended to ensure that individuals inside technology corporations can be prosecuted for refusing to co-operate with a legislative requirements that assist in the investigation or prosecution of online child sexual abuse. The individuals in question should be those that make the decision not to co-operate.

7.2 Removal on online child sexual abuse material

The Synod has been deeply concerned with the evidence that many online businesses are slow to remove illegal content from their platforms, even when they are alerted to it.

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.

[153] Ibid.
[154] Ibid.
[155] Virtual Global Taskforce position on End-to-End Encryption.
[156] Eugene Soltes, 'Why they do it', Public Affairs, USA, 2016, 325.

Survivor of child sexual abuse.[157]

Particularly problematic in failing to co-operate with law enforcement in removing child sexual abuse material online have been image hosts like Imager and TOR, including Depfile. Depfile uses fast fluxing to change IP address rapidly to frustrate the efforts of the police. The child sexual abuse site Playpen was established on TOR.[158]

The hosting of child sexual abuse material online is the result of those in charge of the various online platforms not being vigilant or being complicit. Corporations that host material online can be classed into five groups:[159]

- 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.

Content host corporations often resist removing child sexual abuse images involving children aged 13 to 17.[160]

"We want to remind the industry that these are real children in these photos that they receive notices for. We want people to stop thinking of this as a victimless crime and separate child abuse imagery from pornography. Pornography is consensual between two adults. Child sexual

[157] Canadian Centre for Child Protection, 'Reviewing Child Sexual Abuse Material reporting functions on popular platforms', 2020, 6.
[158] 'Child abuse site creator jailed for 30 years', *BBC News*, 8 May 2017, http://www.bbc.com/news/technology-39844265
[159] Canadian Centre for Child Protection, 'How we are failing children: Changing the paradigm', 2019, 12.
[160] Canadian Centre for Child Protection, 'How we are failing children: Changing the paradigm', 2019, 10.

abuse material is never a choice for that child; it is abuse, and we never agreed to have it shared. The continuous trading of our imagery is a constant burden on our lives. We want governments to stop protecting the rights of these predators over the rights of the innocent children they are destroying. We are demanding that ALL images associated with a child's abuse be removed quickly. Because whether it is a smiling headshot or a tearful action shot, I can tell you firsthand that the smile in the headshot is hiding just as many tears."[161]
Survivor of child sexual abuse responding to technology corporations that refuse to remove or delay removal of child sexual abuse material from their platforms.

The Canadian Centre for Child Protection also reported that some corporations that host content would use any 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.[162]

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.[163]

The Canadian Centre for Child Protection has expressed deep concern that some hosting corporations will refuse to remove all images in a series that documents child sexual abuse. 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. 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. The Canadian Centre for Child Protection argues that the clothed image is still a memorialisation of the child's abuse and should be removed.[164] Such images are typically used to advertise where to find additional images or videos of child sexual abuse.[165]

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.[166] 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.[167]

[161] Ibid., 8.
[162] Canadian Centre for Child Protection, 'How we are Failing Children: Changing the Paradigm', https://protectchildren.ca/en/resources-research/child-rights-framework.
[163] Canadian Centre for Child Protection, 'How we are failing children: Changing the paradigm', 2019, 24.
[164] Canadian Centre for Child Protection, 'How we are Failing Children: Changing the Paradigm', https://protectchildren.ca/en/resources-research/child-rights-framework.
[165] Canadian Centre for Child Protection, 'How we are failing children: Changing the paradigm', 2019, 8.
[166] Canadian Centre for Child Protection, 'Reviewing Child Sexual Abuse Material reporting functions on popular platforms', 2020, 7.
[167] Ibid., 7.

Additional barriers hosting platforms have put in place that hinders the removal of child sexual abuse material are:[168]

- 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
- 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.[169]

Recommendation: Legislation should passed by the Parliament requiring technology providers 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.**

7.3 The need to design the online world for safety

In terms of product design, there is a lack of safeguards for children using the products and a lack of corporations enforcing their own policies. 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.[170] 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.[171] Under the Act, parents can demand that the social media corporation remove the social media site of their child.[172] 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.[173] According to *Consumer Reports,* in 2011, there were 7.5 million children under the age of 13 that had Facebook pages,

[168] Ibid., 8.
[169] Ibid., 12.
[170] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 125.
[171] https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Web%20sites%20and%20online
[172] https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Web%20sites%20and%20online
[173] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 124-125.

and we can safely assume the number has grown since then.[174]

Facebook and Instagram could enforce the age limit policy more effectively, but choose not to. It is reasonable to assume that this is because of the cost that would be involved. When a child opens a Facebook account, they usually start to post photographs of themselves and their friends, who are generally of similar age. They go on to post comments about school, classmates and their activities. A scan of Facebook pages would quickly and easily pick up many of the pages opened by children. 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.[175]

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.[176]

Recommendation: Require that social media corporations cannot allow children under the age of 13 to open accounts on their platforms without verified parental or guardian consent.

7.4 Need to prevent ICT corporations tipping off offenders

The Synod is concerned by ICT corporations that reserve the right to tip off suspected offenders that they are under investigation. Tipping off offenders places victims and witnesses in danger. It also allows an offender to destroy evidence. Often offenders will use multiple platforms and communication devices. Thus, even if data on the platform tipping off the offenders were to be preserved from destruction, after being tipped off, the offender might be able to destroy evidence on other platforms.

The Sheriff's office in Brevard County in Florida reported they had to force entry into a house to stop an alleged child sex offender from continuing to run CDs through a shedder after they were tipped off by an ICT technology corporation that they were under investigation.[177]

Child sex offenders often operate in large online networks that assist each other and will work together to target victims and their families. Thus, the Committee should strongly avoid recommending any measures that would allow a suspected child sex offender they are under investigation, such as being able to contest a warrant needed to pursue an investigation into child sexual abuse where the offender has not already been advised they are under

[174] Ibid., 125.
[175] Ibid., 120-121.
[176] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 8.
[177] https://www.wjhg.com/content/news/Proposed-law-would-stop-internet-service-providers-from-tipping-off-sex-offenders-472270473.html

investigation. Any process that would tip off a suspected child sex offender may also enable them to alert others in their network and possibly seek assistance from others in the network to cover up their activities.

The Synod raises the above concern as civil liberties, human rights and legal bodies regularly advocate for suspected offenders to be tipped off they are under investigation without any regard for the safety of victims, their families, witnesses and the risks of destruction of evidence.

In terms of non-disclosure to a suspected offender or others, the US Department of Justice has instructed US law enforcement agents:[178]

> *Section § 2705(b) states:*
> *A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—*
> *(1) endangering the life or physical safety of an individual;*
> *(2) flight from prosecution;*
> *(3) destruction of or tampering with evidence;*
> *(4) intimidation of potential witnesses; or*
> *(5) otherwise seriously jeopardising an investigation or unduly delaying a trial.*
>
> *This language permits agents to apply for a court order directing network service providers not to disclose the existence of legal process whenever the government itself has no legal duty to notify the customer or subscriber of the process. If the relevant process is a 2703(d) order or 2703 warrant, agents can simply include appropriate language in the application and proposed order or warrant. If agents instead seek to compel the disclosure of information using a subpoena, they must apply separately for this order.*

The EU Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 does require governments to advise suspected offenders when their stored communications and telecommunications data has been accessed under Article 13.[179] However, Article 13 also places limitations on that notification, stating:

> *3. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:*
> *(a) avoid obstructing official or legal inquiries, investigations or procedures;*

[178] US Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 2009. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf accessed 19 February 2020, 140-141.
[179] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
(c) protect public security;
(d) protect national security;
(e) protect the rights and freedoms of others.

Dr Mark Zirnsak
Senior Social Justice Advocate
Phone: [redacted]
E-mail: [redacted]