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

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

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600
E-mail: pjcis@aph.gov.au

Submission by the Synod of Victoria and Tasmania, Uniting Church in Australia to the inquiry into the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*
12 February 2021

The Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes this opportunity to submit to the inquiry into the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*.

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

1. Recommendations

The Synod requests that the Committee makes the following recommendations:

- The *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be passed to give law enforcement agencies vital tools to address serious crimes and human rights abuses facilitated online. The Bill is especially needed in light of technology corporations continuing to develop online tools that assist in carrying out such activities.
- The Australian Federal Police and the Australian Criminal Intelligence Commission must put in place policies, procedures, and best practice guides to ensure full compliance with the requirements and safeguards contained within the Bill.

The Synod supports that protected information collected by the warrants in the Bill can be shared with foreign law enforcement agencies, the International Criminal Court or a War Crimes Tribunal if relevant to an international assistance authorisation. The Synod notes that increasingly those involved in severe organised crime and war crimes operate across borders. The failure of law enforcement agencies to co-operate across borders can result in human rights abuses not being prevented and perpetrators escaping justice.

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 three 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;

3. Assessment Criteria for Regulating the Online World

When considering the regulation of matters related to the online world, the Synod applies the following criteria:

- Does an equivalent existing regulatory power already exist in the offline world? We support platform neutrality, so that regulation of the online world should match regulation that applies across the rest of society.
- Is there any reason why the online world should be treated differently from the offline world on a particular regulation?
- To what extent is the regulatory power or law enforcement tool necessary to prevent human rights abuses, harm to people or the environment?
- Does the proposed regulation have sufficient safeguards against misuse by the regulatory and law enforcement bodies? However, we weigh up safeguards against the impact safeguards have on the effectiveness of the regulatory measure. As an extreme example, in mounting an undercover operation, it could be argued that a safeguard against misuse of undercover operations would be that the organised criminals be told that the police will be planting an undercover officer in their operation and the organised criminals be given the ability to contest the warrant authorising the undercover operation. Obviously, such a safeguard would completely undermine the ability to conduct a covert operation. However, the Synod notes that some civil liberties and human rights organisations have made such arguments when contesting regulation of the online world. For example, they have argued that when police are trying to establish the identity of a person that has repeatedly participated in an online child sexual abuse network, the person in question should be alerted and should be able to contest through the courts the ability of the police to establish their identity.
- Is there a level of malicious misuse of any existing equivalent regulation by regulators or law enforcement agencies that would cause the Synod to be concerned about granting the power to a regulator or law enforcement agency? That involves weighing up the level of misuse against the level of legitimate use. It also means assessing the harm to people due to the misuse of the powers compared to the harm that will result to people if law enforcement agencies do not have access to the powers.

In the case of the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, the Synod notes that surveillance and covert operations by law enforcement agencies of severe crimes are already permitted in the offline world. Such controlled, undercover operations appear to be an essential tool in law enforcement agencies' ability to curb serious organised crime. The Synod cannot see why similar surveillance and covert operations should not be permitted in the online world with similar safeguards over their use. It is not apparent to the Synod why those suspected of serious criminal activity that would involve the harm of people should be afforded greater protection from being investigated in the online world than the rights provided to them in the offline world.

4. 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.

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

The UNODC has argued that "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 that 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.*
>
> *Article 36*
> *States Parties shall protect the child against all other forms of exploitation prejudicial to any aspects of the child's welfare.*

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

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, if and 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:

> *"…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*

[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.

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 emphasised 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.

At times, the powers granted in the Bill will assist law enforcement agencies to protect the privacy of victims of human rights abuses. For example, law enforcement agencies may be able to delete child sexual abuse material or block access to online locations containing child sexual abuse material, protecting the victims' privacy rights. Law enforcement agencies may disrupt or delete the use of malware that would violate the privacy of potential victims of serious crimes, such as a case where a perpetrator is using the online world to facilitate family violence. In 2018, Women's Aid in the UK reported that 29% of family violence survivors reported being subjected to the "use of spyware or GPS locators".[7] WESNET was quoted in the media in August 2019 stating they received about two inquires a week from women dealing with family violence who suspected, or discovered, they had spyware installed on their phone.[8] In July 2020, Computer Weekly reported that the use of spyware and stalkerware was up more than 50%, with a clear link to a spike in domestic violence in the UK.[9] Stalkerware may give a user the ability to track their victim's location, access personal data such as photos and videos, intercept e-mails, texts and app-based communications, eavesdrop on phone calls and record conversations.

Researchers from Deakin University reported in 2019 that spyware was available for general consumption within Australia. Multiple products can be used to capture SMS message data from a phone, make voice-recordings of phone conversations, capture internet browsing history, access private videos or photos, allow live access to the phone's camera, and microphone. Certain spyware products also contain the ability to send 'spoofed' SMS messages that assume a captured device's identity. All of the above can be done without the knowledge of the targeted device's owner.[10] The researchers reported that companies selling spyware market it as suitable for use targeting intimate partners and children, making it an acute threat in the context of family violence.[11]

[7] Adam Molnar and Diarmaid Harkin, 'The Consumer Spyware Industry. An Australian-based analysis of the threats of consumer spyware', Deakin University and the Australian Communications Consumer Action Network, 2019, 3.
[8] Alison Branley and Loretta Florance, 'How companies selling spyware are helping to promote family violence', ABC News, 22 August 2019.
[9] Alex Scroxton, 'Use of spyware apps linked to domestic abuse soars in lockdown', Computer Weekly, 8 July 2020.
[10] Adam Molnar and Diarmaid Harkin, 'The Consumer Spyware Industry. An Australian-based analysis of the threats of consumer spyware', Deakin University and the Australian Communications Consumer Action Network, 2019, 1.
[11] Ibid., 1, 11-14.

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 serious human rights abuses and crimes 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.

The Synod is of the view the law enforcement tools and powers contained in the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, with the safeguards against their misuse, are justified to allow law enforcement agencies to prevent severe human rights abuses.

5. Assessing the Risks of Misuse of the Powers in the Bill

In assessing if Australian law enforcement agencies have maliciously misused the covert powers granted to them, the Synod considered the Commonwealth Ombudsman assessments.

The latest Commonwealth Ombudsman report assessing the use of controlled operations by the Australian Federal Police and the Australian Criminal Intelligence Commission (ACIC) between 1 July 2019 and 30 June 2020 found both agencies were generally compliant with the legislative requirements of such operations. The number of compliance findings in high-risk areas decreased compared to 2018 – 2019, particularly regarding unauthorised conduct and participants.[12] Issues of concern raised by the Commonwealth Ombudsman with regards to the ACIC were:[13]

- Three instances where it was not clear whether activities that participants were engaged in during a controlled operation were authorised;
- One instance where the principal law enforcement officer was not listed as a law enforcement participant on the controlled operation authority;
- One written record did not accurately reflect the approved conduct; and
- Issues related to the general register and other record-keeping matters.

The Commonwealth Ombudsman pointed out that where an authority for a controlled operation does not specify the authorised conduct, it can create ambiguity about what conduct is authorised. As a result, there will be an increased risk of unauthorised conduct and exposure to civil and criminal liability.[14]

Concerning the Commonwealth Ombudsman's assessment of the Australian Federal Police compliance with controlled operations requirements, they examined 27 of 48 controlled operations that expired or were cancelled between 1 January and 30 June 2019.[15] They reported:[16]

- Four instances where they were unable to determine from the AFP records whether civilian participants' conduct was appropriately authorised and indemnified. The Commonwealth Ombudsman stated they did not consider these instances are representative of a systemic problem.
- Several applications for controlled operations authorities did not include an explicit statement that the nature and extent of the criminal activity justified using a controlled operation or that any controlled conduct would be limited to the maximum extent possible.
- One instance where a written record of an urgent variation application did not explicitly identify why the delay anticipated in making a formal application may affect the controlled operation's success.
- The AFP's general register did not include all the fields that were required by the legislation.
- The AFP's six-monthly report for the period 1 January to 30 June 2019 contained three errors. In two instances the report did not include the identity of all persons targeted, and in

[12] Commonwealth Ombudsman, 'A report of the Commonwealth Ombudsman's activities in monitoring controlled operations for the period 1 July 2019 to 30 June 2020', 9 December 2020, 2.
[13] Ibid., 6-8.
[14] Ibid., 12.
[15] Ibid., 15.
[16] Ibid., 15, 18-22.

one instance the date of the application for an urgent variation was not specified. The Commonwealth Ombudsman stated that they consider the AFP has adequate processes to achieve compliance with the legislation's reporting requirements despite these instances.

While the Synod is concerned by the examples of non-compliance by the ACIC and AFP with legislative requirements for controlled operations, the Commonwealth Ombudsman did not find any examples of intentional misuse of controlled operations or highlight cases of harm that resulted from the instances of non-compliance. The Synod, therefore, takes the view that the Committee should recommend that law enforcement agencies able to access the tools contained in the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* be required to put in place policies, procedures and best practice guides to ensure full compliance with the requirements and safeguards contained within the Bill.

Similarly, the Commonwealth Ombudsman's latest assessment of law enforcement agencies access to stored communications and telecommunications data under Chapters 3 and 4 of the *Telecommunications (Interception and Access) Act 1979* identified areas at some agencies where further work was needed to satisfy the Act's requirements adequately.[17] Further, several issues identified by the Commonwealth Ombudsman in 2017-2018 were again identified in the 2018-2019 inspections. While some of these were due to the inspections' retrospective nature, in some instances, the agencies had not taken adequate remedial action to address the previous findings of the Ombudsman.[18] The Commonwealth Ombudsman recommended that there be more robust compliance controls. Simultaneously, the Commonwealth Ombudsman stated they saw a high level of responsiveness to the Ombudsman's inspection findings.[19] It should be noted that the findings of the Commonwealth Ombudsman in the report applied to law enforcement agencies that are not covered by the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*. For example, the Commonwealth Ombudsman reported that the Tasmanian Police did not have a well-developed compliance culture.[20]

Regarding the ACIC the Commonwealth Ombudsman found four instances where the ACIC gave preservation notices after it had already issued the telecommunications warrants it intended to rely on to access the stored communications. The ACIC stated it issued the preservation notices to ensure the carrier did not destroy the stored communications they needed to access.[21]

Concerning the AFP, the Commonwealth Ombudsman reported that the AFP had continued to give successive foreign preservation notices despite the issue being raised with them by the Commonwealth Ombudsman in its 2017 – 2018 inspections.[22] The AFP had also applied for a warrant to access the stored communications of a victim of a serious contravention. There were no records on file to indicate the victim was unable to consent or it was impracticable for the AFP to obtain their consent.[23] The Commonwealth Ombudsman identified instances where the

[17] Commonwealth Ombudsman, 'Monitoring agency access to stored communications and telecommunications data under Chapters 3 and 4 of the *Telecommunications (Interception and Access) Act 1979.* For the period 1 July 2018 to 30 June 2019', 2020, 7.
[18] Ibid., 7.
[19] Ibid., 7.
[20] Ibid., 13.
[21] Ibid., 22.
[22] Ibid., 23.
[23] Ibid., 24.

AFP had not destroyed stored communications information forthwith, contrary to Section 150(1) of the *Telecommunications (Interception and Access) Act 1979*.[24] The Commonwealth Ombudsman also identified where the AFP had sent correspondence to a carrier which directed it to:

- Retain preserved stored communications even though a foreign preservation notice was not in force; and
- Release preserved stored communications in the absence of a stored communications warrant.

There were no records to indicate the carrier had acted on the AFP's directions. The AFP confirmed the carrier did not provide any stored communications information as a result of the correspondence.[25] The Commonwealth Ombudsman also concluded that AFP authorised officers did not have a consistent practice for documenting their considerations when making an authorisation to access telecommunications data.[26]

Again, the Synod is concerned by the instances of non-compliance with legislative requirements in accessing stored communications and telecommunication data outlined by the Commonwealth Ombudsman. However, none of the instances outlined indicated deliberate misuse of the powers available to the ACIC or AFP and the Commonwealth Ombudsman gave no examples of harm resulting. As a result, the Committee should grant the additional powers and tools to the ACIC and AFP in the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020.* At the same time, it should recommend that the ACIC and AFP be required to put in place policies, procedures and best practice guides to ensure full compliance with the requirements and safeguards contained within the Bill.

[24] Ibid., 24.
[25] Ibid., 24.
[26] Ibid., 47.

6. Disruption Warrants

The Synod supports the data disruption warrants, significantly so that law enforcement agencies will be able to prevent online crimes from continuing. Such powers are important due to the lack of co-operation by many technology corporations with law enforcement agencies and their lack of pro-active efforts to ensure their services are not being used to facilitate serious human rights abuses or crimes.

Taking the example of online child sexual exploitation, 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. When platforms don't actively look for or prevent this content from being uploaded, the burden falls to me to have these images removed. Each time one account gets taken down, five more like it take its place. It's like a hydra, a monster that I can never defeat. I'm not strong enough to take it down myself. It's costing me my well-being, safety and maybe even my life. I'm tired. I shouldn't find photos of myself as a child being raped when I'm just scrolling through my feed.*
> Survivor of child sexual abuse.[27]

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.[28]

This discretion means these corporations determine, at least in part, government agencies access to information about our personal relationships, professional engagements, travel patterns and financial circumstances. At the same time, they impact the government's ability to prevent terrorism, the rape of children, solve murders and locate missing children. These corporations are now responsible for decisions that have significant consequences for our privacy on the one hand, and our safety and well-being on the other.[29]

US technology corporations not taking responsibility for what is posted on their platforms has been assisted by US law. 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 to be a "publisher or speaker". [30]

Particularly problematic in failing to co-operate with law enforcement in removing child sexual

[27] Canadian Centre for Child Protection, 'Reviewing Child Sexual Abuse Material reporting functions on popular platforms', 2020, 6.
[28] '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.
[29] Ibid.
[30] Harcher, P., 'Taming big tech's titans', *The Age*, 25 February 2020, 20.

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.[31]

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.[32]

> *"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 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."*[33]
> 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 will 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.[34]

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.[35]

---

[31] 'Child abuse site creator jailed for 30 years', *BBC News*, 8 May 2017, http://www.bbc.com/news/technology-39844265
[32] Canadian Centre for Child Protection, 'How we are failing children: Changing the paradigm', 2019, 10.
[33] Ibid., 8.
[34] Canadian Centre for Child Protection, 'How we are Failing Children: Changing the Paradigm', https://protectchildren.ca/en/resources-research/child-rights-framework.
[35] Canadian Centre for Child Protection, 'How we are failing children: Changing the paradigm', 2019, 24.

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

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

- Reporting structures that create strong disincentives for users to report illegal content, such as requirements to provide personal contact information;
- The inability to report publicly visible content without first creating (or logging onto) an account on the platform;
- Difficulty locating reporting tools on the interface, with, at times, inconsistent navigation between desktop and mobile versions of the platform; and
- The inability to report specific users, user profiles, specific posts, or a combination of the latter.

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

In addition to online child sexual abuse, the Synod is aware of criminal activity for sale online. Criminal activities can be ordered and purchased online from services offering to carry out extortion, scams and assassinations. There are also online sites selling stolen credit card details, illicit drugs and illegal weapons. The websites selling these criminal activities often have shopping carts, concierge hospitality, and excellent customer service.[40] The sites offer discount days, coupon codes, two-for-one specials, money-back guarantees, and loyalty points. Promotional campaigns are frequent, and some drug-trading sites provide escrow services; they will hold the customer's money until their package arrives safely.[41]

Customers are asked about their level of satisfaction and given opportunities to offer suggestions for improvement.[42]

McDumpals is one of the leading sites that sell stolen credit card details. Its logo is golden arches with the motto "I'm swipin' it". It has a gangster version of Ronald McDonald as its mascot.[43]

[36] Canadian Centre for Child Protection, 'Reviewing Child Sexual Abuse Material reporting functions on popular platforms', 2020, 7.
[37] Ibid., 7.
[38] Ibid., 8.
[39] Ibid., 12.
[40] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 262.
[41] Ibid., 268.
[42] Ibid., 268.
[43] Ibid., 269.

Another site selling stolen credit card data is Uncle Sam's dumps shop. It encourages buyers to "Make credit card fraud great again".[44]

One site selling paid murders boasts "I always give my best to make it look like an accident or suicide". Another states "The best place to put your problems is in the grave". Some of the sites selling murders offer a chance to win back some of the cost if the buyer can guess the assassination's time.[45]

The way these criminal businesses operate online demonstrates that law enforcement agencies currently lack both the powers and the resources needed to end the severe harms many of these businesses cause.

Section 43C (4) is necessary as it can be arbitrary where a technology corporation decides data is located. Thus, a disruption warrant should not be frustrated because the location where the data is held is unknown or cannot be reasonably be determined.

[44] Kerbs on Security, 'Trump's Dumps: 'Making Dumps Great Again', 26 May 2017.
[45] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 269.

7. Network Activity Warrants

The Synod supports the need for network activity warrants to counter the 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).[46] Those engaged in child sexual abuse online teach each other how to become anonymous online.[47] They are more commonly educating each other on using private chats, Internet voice and video chat software, forums and anonymisation software.[48] The feeling of impunity, as a result of those carrying out the abuse being able to conceal their identity, has enabled them to diversify their activities.[49]

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.[50] Child sexual abuse sites on the darknet are particularly being used by offenders to host and distribute sexual abuse material involving infants and toddlers.[51] 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.[52] A forum dedicated to discussing the abuse of children exceeded 23 million visits.[53] On another darknet site, each user uploaded one three minute video or two images each month of child sexual abuse as membership payment.[54]

Child sexual abuse perpetrators operate in networks online to assist each other. 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.[55]

Currently, most reports of child sexual abuse material online come from major technology corporations. In 2019, Facebook made 15.9 million (94%) of the reports to the US National Center for Missing and Exploited Children.[56] Google provided 449,283 of the reports (2.7%).[57] Only 150,667 reports (0.89%) of online child sexual abuse reported to the US National Center

[46] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 5, 15.
[47] Ibid., 15.
[48] Ibid., 16.
[49] Ibid., 5.
[50] Internet Watch Foundation, 'IWF Annual Report 2016', 13 and Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', 20.
[51] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 16.
[52] Ibid., 16.
[53] Ibid., 16.
[54] Ibid., 16.
[55] Ibid., 15.
[56] US National Center for Missing and Exploited Children, '2019 Reports by Electronic Service Providers (ESP)', 2020, 2.
[57] Ibid., 2.

for Missing and Exploited Children came from members of the public.[58]

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.[59] These threats of changes in online technology corporations' behaviour increase the need for law enforcement to be given effective tools to respond, such as network activity warrants.

Section 43E (3) is necessary as it can be arbitrary where a technology corporation decides data is located. Thus, a network activity warrant should not be frustrated because the location where the data is held is unknown or cannot be reasonably be determined.

[58] US National Center for Missing and Exploited Children, https://www missingkids.org/footer/media/keyfacts
[59] 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

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

8.Controlled Operations

The Synod notes that Schedule 4 of the Bill to enhance the ability of the AFP and ACIC to conduct controlled operations online is consistent with their ability to conduct controlled operations in the physical world offline.

Dr Mark Zirnsak
Senior Social Justice Advocate
[redacted]