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

Centre for Theology and Ministry
29 College Crescent
Parkville Victoria
Australia, 3052
Telephone: +61-3-9340 8807
jim@victas.uca.org.au

Electronic Surveillance Reform Branch
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

Submission by the Synod of Victoria and Tasmania, Uniting Church in Australia in response to 'Reform of Australia's electronic surveillance framework' Discussion paper 11 February 2022

The Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes this opportunity to make a submission to the 'Reform of Australia's electronic surveillance framework' Discussion Paper.

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

The Synod's response to the discussion paper is shaped by the resolution adopted by the Synod meeting of hundreds 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. Are there any additional agencies that should have powers to access particular information and data to perform their functions? If so, which agencies and why?

The Synod strongly supports AUSTRAC, the ATO, Australian Border Force and state and territory corrective services being additional agencies that should be able to obtain warrants and authorisations to use electronic surveillance and access online and stored information to pursue their legitimate law enforcement functions.

We would also support the enforcement arm of the Department of Agriculture, Water and Environment also being granted the ability to obtain warrants and authorisations to use electronic surveillance to investigate cases of illegal logging covered by the *Illegal Logging Prohibition Act.* The importation of illegally logged timber or wood products carries a maximum sentence of five years imprisonment under the Act. Support for the enforcement arm of the Department having these powers, if they would be helpful, is due to the complexity of illegal logging cases taking place overseas and supplying product into Australia. Illegal logging is usually associated with serious corruption, especially bribery. Other crimes associated with illegal logging are tax evasion and in a few cases murders of government officials and environmental defenders that seek to expose the illegal logging operations.

The UN Office on Drugs and Crime reported in 2019 that "corrupted licences given to plantation firms in Indonesia are among the main underlying causes of Indonesia's deforestation."[1] They indicated that "examples of common corruption schemes included falsified origin of logs being cut in protected forests, invalid Environmental Impact Assessments, or falsified numbers of logs or size of the area authorised for plantations."[2]

INTERPOL has reported that organised criminals collectively make more than $200 million a year from illegal logging from tropical forests.[3] These operations often occur hand-in-hand with other criminal activity, such as document fraud, money laundering, violence, intimidation and

[1] UNODC, 'UNODC and KPK pilot a Corruption Risk Assessment in the Forestry Sector in South-Sumatra Province, Indonesia', 11 January 2019.
[2] Ibid.
[3] INTERPOL, 'International Day of Forests: protecting Earth's most biologically diverse ecosystems', 20 March 2020.

murder.[4] A 2016 review of INTERPOL's databases found that the most common corruption offences associated with forestry crime were, in order of most to least common, were bribery, fraud, abuse of office, extortion, cronyism and nepotism.[5] INTERPOL reported that between 2009 and 2014, a 13 country survey identified an average of 250 cases of corruption related to the forestry sector, per year per country.[6]

4. Do you agree with the proposed considerations for determining whether additional agencies should be permitted to access peoples' information and data? Are there any additional considerations that have not been outlined above?

The Synod supports the proposed list of considerations for determining whether additional agencies should be permitted to access people's information and data. An additional factor that could be considered is the urgency the agency is likely to need to be able to gather information to prevent serious harm from happening or rescuing a victim from further severe abuse. However, it might be argued such consideration would already be a factor in a public interest test for the agency to have the powers.

8. What kinds of information should be defined as 'content' information? What kinds of information should be defined as 'non-content information'?

The Synod would support 'content' information being anything the person has created or generated. That would include any message or draft message, even when that message might be forwarding or posting something that someone else has generated or created. 'Non-content' information would include metadata and any information about communication or online activity that the person has not generated or created themselves. Thus, the URLs a person has visited would be 'non-content' information, as it only reveals what a person has viewed. Given the material hosted at the URL is highly likely to be accessible to multiple people, it is not private information that relates to the person viewing it. Such URL history may be of great assistance in helping law enforcement identify if the person is likely to be a person of interest in an investigation, for which warrants might be necessary to gain access to their content information. URL history might expose if the person has been accessing child sexual abuse material or visiting sites that reveal they are likely to have been researching how to carry out a serious crime.

However, counter to this view, we note that if police wanted to access the borrowing history of someone from a public library, which might also reveal if they were researching how to commit a serious crime, they would need a court issued warrant. Thus, it is also a valid point of view to argue that a court issued warrant should be required to access a person's URL browsing history.

11. Should the distinction between 'live' and 'stored' communication be maintained in the new framework?

As highlighted by the discussion paper there is little reason to now treat 'live' and 'stored' communication differently. Thus, the distinction should no longer be maintained in the new framework.

[4] Ibid.
[5] INTERPOL, 'Uncovering the Risk of Corruption in the Forestry Sector', 9 December 2016, 1.
[6] Ibid, 1.

12. Do each of these kinds of information involve the same intrusion into privacy? Or should the impact of each be considered differently?
In the Synod's view, access to both 'live' and 'stored' communication should be subject to the same privacy considerations and protections.

13. What type of Australian communication providers should have obligations to protect and retain information, and comply with warrants, authorisations and assistance orders under the new framework?
The Synod believes that the principle that should apply is that there should be no avenue of electronic communication where law enforcement agencies are unable to access the communications. Any communication platform that is not accessible to law enforcement agencies will be highly attractive to those that need electronic communication to carry severe human rights abuses and serious crimes. Thus, it may not be necessary for every communication provider to have to protect and retain information, and comply with warrants, authorisations and assistance orders if there are multiple different types of providers in a communication chain. However, any provider that may be the only provider in a communication chain must be subject to the obligations.

14. What are your thoughts on the above proposed approach? In particular, how do you think the information captured by surveillance and tracking devices could be explained or defined?
The Synod would support an approach that would regulate the use of surveillance devices by the sensitivity of the information to be collected and the level of intrusion needed to set up or install the device. The Synod would support the current regime of allowing a tracking device to be used under internal authorisation where the use of the device does not involve entry onto premises or interference with the interior of a vehicle without the owner's permission. Internal authorisation should also apply to optical and listening devices where they will capture activity taking place in public settings.

A warrant should be required where the surveillance device will capture the content of a private communication, such as a conversation in a private residence or private vehicle. A warrant should be required where the surveillance device will capture the content of electronic communication.

15. How could the current warrant framework be simplified to reflect the functional equivalency of many of the existing warrants while ensuring appropriate privacy protections are maintained?
The Synod supports the proposed direction of the paper. The number of warrants should be simplified to reflect the type of information to be accessed, rather than the method by which the access can be obtained. The court should then assess the proposed methods to be used to access the information and authorise which methods can be applied by considering factors including:

- the seriousness of the offences being investigated;
- the urgency in which law enforcement need the information to prevent more offending or ensure that a prosecution will be possible, and;
- if less intrusive methods could be used to obtain the information in the required timeframe.

17. Is it appropriate to harmonise legislative thresholds (as outlined above) for covert access to private communications, content data and surveillance information where existing warrants are functionally equivalent?

The Synod agrees that it is appropriate to harmonise legislative thresholds for covert access to private communications, content data and surveillance information. The values that underlie where the threshold are set is a comparison between the seriousness of the criminal activity and the harm it is likely to cause if left unaddressed against the level of intrusion needed to obtain the evidence to determine if the offence is taking place. Where law enforcement agencies are allowed to use methods for covert access the decision is that the seriousness of the harm justifies the use of the covert method. Where law enforcement is denied access to covert methods the consequence is that the potential harm the offender may inflict is not sufficiently serious that the use of a covert method is justified.

The threshold of penalty for the use of covert methods also results in an outcome where offenders who have access to technological expertise are more likely to escape detection and prosecution for crimes below the threshold set, potentially allowing the criminal behaviour and associated human rights abuses to persist for those crimes. It is likely offenders that have access to technological expertise are those that are more organized and are committing offences at the more serious end of the scale for that particular crime.

The Synod would prefer the default threshold be set at the level identified by Article 2(b) of the *UN Convention against Transnational Organised Crime* definition of serious crime as:

> *(b) "Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty;*

Australia is a State Party to the Convention.

Additional offences below the four-year imprisonment threshold should be included where the seriousness of the potential harm caused by the offending would justify the use of covert methods to prevent that harm.

As noted in the consultation paper s.478.1(1) of the *Criminal Code* for unauthorised access to, or modification of, restricted data, only carries a maximum penalty of two years in prison. Such criminal activity may point to far more serious criminal activity behind the unauthorised access.

As another example, the unlawful removal of a child from Australia under s. 65Y of the *Family Law Act* can cause great distress to both the children and the parent who does not know where the children have been removed to. Australia has obligations under the Hague Convention on the Civil Aspects of International Child Abduction. The situations where the unlawful removal of a child from Australia by one parent can occur are complex. Such unlawful removals of children from Australia may be a violation of the human rights of the children in question. It is our understanding that the AFP almost never seek a prosecution under s. 65Y as it is usually not in the best interests of children to have their parent imprisoned. However, it is further to our understanding that there are cases where one parent removes the children from Australia and places them in the care of relatives overseas as a means to cause distress on the other parent, as a form of emotional family violence. We would therefore take the view that there may be circumstances where the AFP should be able to use covert methods to locate children who have been removed overseas, especially where the safety or well-being of the children is under threat. There are likely to be other circumstances, such as the parent who unlawfully removes

the children from Australia is doing so to escape family violence being perpetrated against them and the children, where it would not be appropriate for the AFP to assist in the location of the children. The point being, that the complexity of the situations that may arise can justify covert methods being available for some rare cases. The Senate Legal and Constitutional Committee conducted an inquiry into this issue in 2011, highlighting the distress and suffering that unlawful removal of children from Australia can cause.[7]

18. Are there any other changes that should be made to the framework for accessing this type of data?

The Synod supports that the existing system of access to metadata by law enforcement agencies investigating serious crimes, many of which are also severe human rights abuses, be maintained while addressing the issues identified by the Commonwealth Ombudsman:

- Establishing a formal framework for law enforcement agencies to verbally issue authorisations for access to telecommunications data in urgent out-of-hours cases;
- Formal procedures around the storage of telecommunications data obtained by law enforcement agencies;
- Formal procedures for the destruction of telecommunications data obtained by law enforcement agencies and for length of retention before destruction;
- Clarification on what constitutes 'content'; and
- Clarification on when a revocation of an authorisation takes effect.

The Synod strongly urges that there be no introduction of measures that will tip off suspected offenders they are under investigation. There is a need to avoid tipping off suspected offenders to prevent them being able to destroy evidence (both in the physical world and across multiple platforms), tip off other offenders, intimidate victims and witnesses or seek to bribe the family of a child sexual abuse victim to not co-operate in an investigation. These are all activities that some child sexual abuse offenders will undertake if given early warning of an investigation, such as being tipped off that a warrant has been applied for. Child sexual abuse offenders often collaborate in large online networks, assisted by the anonymity that the online world provides them.

Any additional impediments to law enforcement access to metadata will reduce the number of cases that law enforcement can conduct, meaning less victims rescued from on-going serious harm and there is a further erosion of general deterrence. General deterrence is eroded when law enforcement agencies are subjected to restrictions and impediments that increase the perception amongst offenders that they will be able to get away with the harm they are inflicting on others. Reducing the number of cases law enforcement agencies are able to work on will increase the perception that there is less risk of being caught and sanctioned.

Impeding access to metadata means that for the same level of law enforcement resources less cases can be investigated. Increasing the role of courts in having to issue warrants would take up more time before the courts and is likely to further impede law enforcement investigations as there are further delays in the issuing of warrants.

7 https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Completed_inquiries/2010-13/childabduction/report/index

The Virtual Global Taskforce reported that a joint report between Online Child Exploitation Across New Zealand (OCEANZ) and the New Zealand Police, *Online Child Exploitation: Emerging Trends and the Pacific. Intelligence Report,* reported that data preservation and data retention created challenges to investigations into online child sexual abuse due to the data retention practices and policies of ISPs.[8]

The Synod is also of the view that the Australian Taxation Office should be a law enforcement agency to have access to telecommunications data and stored communications in its efforts to curb tax evasion and tax avoidance.

Canada provides an example of law enforcement agencies having investigations frustrated by not having a simple system to access subscriber data without a court warrant. In Canada police may need to obtain a judicial authorisation signed by a judge to have an Internet Service Provider provide police with subscriber data if the provider refuses to co-operate with police.[9] The requirement reportedly significantly reduced the number of cases of online child sexual abuse that Canadian police are able to investigate.[10]

Historically, subscriber data has been made available by Canadian service providers without prior judicial authorisation (such as a search warrant).The Supreme Court of Canada decision in *R v. Plant*, (1993) 3 S.C.R 281, held that, in the context of information held by a business, a person does not have a reasonable expectation of privacy in personal information that does not tend to reveal intimate details of their lifestyle and personal choices. The *Personal Information Protection and Electronic Documents Act* allows for the disclosure of personal information without the knowledge and consent of the individual to whom it pertains. Such disclosure can only be made to a government institution that has identified its lawful authority to obtain such information.[11]

In 2014, the Supreme Court of Canada ruled that police were required to have a search warrant to get the name and address of a person associated with an IP address.[12]

In the 2014 case considered by the Supreme Court of Canada, the offender had downloaded child sexual abuse material and placed it in a folder accessible to other Internet users using the same file-sharing program.[13] Being able to identify the offender from their IP address allowed the police to apprehend the offender who was subsequently convicted at trial of possession of child sexual abuse material and acquitted on a charge of making it available.[14] In the appeal the defence team did not argue that the defendant did not access child sexual abuse material, but rather he had a right to expect the ISP would conceal his identity from police as part of his right to privacy.[15] The Supreme Court of Canada did rule that a person engaged in online child sexual abuse should have a reasonable expectation of privacy in their subscriber information and that a police request for an ISP to voluntarily disclose such information amounted to a

[8] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 25.
[9] https://www.justice.gc.ca/eng/cons/la-al/d.html
[10] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 5.
[11] https://www.justice.gc.ca/eng/cons/la-al/d.html
[12] https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do
[13] Ibid.
[14] Ibid.
[15] Ibid.

search.[16] Fortunately, the court dismissed the appeal and upheld the conviction. The court ruled that while the police should have obtained a warrant to access the offender's subscriber data to identify him, police had acted in good faith and the administration of justice would be impaired if the broader evidence gathered by police were thrown out of court.[17]

If the service provider holding the subscriber information does not wish to cooperate with law enforcement agencies, then the law enforcement agency requires a court order. The Canadian Government has stated in September 2021 that a problem exists in cases where no warrant can be obtained under the *Criminal Code* (such as s. 487) because law enforcement agencies may require the information for non-investigatory purposes (for example, to locate next-of-kin in emergency situations) or because they are at the early stages of an investigation.[18]

Even in 2012, Canadian Association of Chiefs of Police expressed concern about their inability to have warrantless access to basic subscriber data. They stated "lack of timely access to such information can, and often does, block investigations."[19]

In 2010, the Royal Canadian Mounted Police's National Child Exploitation Coordination Centre reported that the average response time to obtain basic subscriber data was 12 days and the information was only provided in 72.5% of the time.[20] In 18.2% of cases the provider did not have basic subscriber data about the user.[21]

The Canadian Association of Chiefs of Police expressed concern that in the case of missing persons, police often do not have obvious grounds that a crime is involved, or that it is urgent. They feared a court would not issue warrants in such cases, yet the first 24 hours of a missing person investigation are crucial.[22]

In December 2010, the New Brunswick Royal Canadian Mounted Police began an investigation a case of peer-to-peer sharing of child sexual abuse material. Police suspected that up to 170 IP addresses were associated with a single offender. Police applied to the court for a warrant to obtain the basic subscriber data about the user from the online service provider. The basic subscriber data was provided 15 days later, by which time the offender had ceased their Internet activity.[23] They were subsequently arrested when they recommenced their online activity ten months later.[24]

In 2007, the Royal Canadian Mounted Police assisted in an international investigation in which suspects located in Canada were attempting to defraud American corporations of approximately $110 million. The investigation required police to find the individuals who were accessing unsecured wireless computer networks in the Toronto area to commit the fraudulent activities. The suspects were constantly on the move and police needed the immediate support of telecommunications service providers to locate the networks. The service providers refused to

[16] Ibid.
[17] CBC News, 'Internet users' privacy upheld by Canada's top court', 14 June 2014.
[18] https://www.justice.gc.ca/eng/cons/la-al/d.html
[19] Canadian Association of Chiefs of Police, 'Simplifying lawful Access – Bill – C-30 – Through the Lens of Law Enforcement', 5.
[20] Ibid., 5.
[21] Ibid., 12.
[22] Ibid., 6.
[23] Ibid., 12.
[24] Ibid., 12.

cooperate. As a result police were required to allocate eight full-time technical investigators for five days to finally locate and arrest the suspects. The offenders had successfully defrauded victims of $16.5 million. If police had been able to immediately compel the cooperation of the telecommunications service providers the loss from the fraud would have been less and the level of police resources for the operation would have been greatly reduced. [25]

19. What are your views on the proposed thresholds in relation to access to information about a person's location or movements?
The Synod would support the threshold for being able to use a tracking device remain related to offences punishable by a maximum of three years in prison. There should be the ability to include additional offences to which tracking devices can be used where the likely harm from the offence would justify the use of the tracking device even if the maximum penalty under law is less than three years in prison.

The Synod supports the ability to track an object or premises for the investigation of crimes that have a maximum penalty of three years in prison.

The Synod supports that law enforcement agencies have the ability to internally authorise the use of certain tracking devices where using the device does not involve entry onto premises without permission or interference with the interior of a vehicle without the permission of the owner.

20. What are your views on the proposed framework requiring warrants and authorisations to target a person in the first instance (with exceptions for objects and premises where required)?
The Synod supports that warrants and authorisations should target a person in the first instance, where possible. However, it is essential to be able to issue warrants and authorisations in relation to objects and premises where the likely harm would justify the use of such a warrant and there was no effective and practical alternative available. An example, as mentioned in the discussion paper, would be the ability to obtain a warrant to search a computer distributing child sexual abuse material even if the user of the computer is unknown.

21. Is the proposed additional warrant threshold for third parties appropriate?
The Synod supports the ability to obtain warrants for the surveillance of third parties where that is necessary, given the seriousness of the harm that may otherwise result. We support that the issuing authority be required to demonstrate that alternatives to the warrant targeting the third party would be impractical or ineffective.

There is substantial complexity to defining unrelated third parties. The reality is that there is spectrum of the ways people may be connected to criminal activity and human rights abuses facilitated online. The spectrum can include:

- The offender;
- A person knowingly facilitating the actions of the offender;
- A person recklessly or negligently facilitating the actions of the offender, but who may lack knowledge of the offending or human rights abuses and may not be guilty of an offence themselves through their behaviour;

[25] Ibid., 13.

- A person who has been deceived into assisting the offender in their activities and who may have no knowledge of the offending or human rights abuses;
- A person whose identity has been stolen and is being used to carry out the criminal activity. In some cases the person's computer may also be hijacked without their knowledge and used to perpetrate serious crimes and human rights abuses; and
- Innocent third parties that have no association with the crime or human rights abuses associated with the criminal activity.

Thus, it may be reasonable for a court to consider the likely culpability of the third party in the criminal activity as a factor in deciding to grant a warrant relating to that third party. The greatly the likelihood the person has knowingly, recklessly or negligently been involved with or facilitated the criminal activity the greater the weight the court should give in granting the warrant regarding the third party.

There has been an on-going trend of people involved in serious crime to use shell companies with straw directors and dummy owners to launder the proceeds of crime and facilitate other criminal conduct. As examples of such cases, the ATO and AFP obtained the conviction of Philip Northam to six years in prison for tax evasion related offences in 2020. Australian companies were stripped of their assets and left in a position where they were unable to pay their tax debts. Once the assets of the company were stripped, new straw directors and shareholders were put in place before the company was wound up. The joint ATO and AFP investigation was able to recover $4.5 million of lost government revenue from the criminal conduct.[26]

In the case of the Plutus Payroll fraud the criminals involved set up a significant number of shell companies with straw directors. One of the criminals involved had a full-time role to manage and control the straw directors.[27] Plutus issued false invoices to the shell companies and siphon out the PAYG not paid on behalf of the client companies using its payroll service.[28] To try to escape action by the ATO, the shell companies would be wound up and replaced with a new shell company with a new straw director.[29] It was found that Devyn Hammond would sign off on records in place of the straw directors and impersonate them in e-mails.[30] The scheme allegedly defrauded the Commonwealth Government of $105 million over three years.[31] As of July 2020, 16 people had been charged in relation to the criminal conduct and five had been sentenced to prison.[32] It is possible that a number of the straw directors were not aware of criminal activity being carried out. Assessment of the case suggests that the investigation lasted for as long as it did because the law enforcement agencies were frustrated in being able to establish the link between the criminals behind the scheme and the straw directors.[33]

[26] ATO, '19-year tax fraud probe ends in jail time for scheme promoter', 17 August 2020, https://www.ato.gov.au/Media-centre/Media-releases/19-year-tax-fraud-probe-ends-in-jail-time-for-scheme-promoter/
[27] Cactus Consulting, 'Plutus Payroll Case Study; Significant tax fraud', 26 November 2019.
[28] Ibid.
[29] Cactus Consulting, 'Plutus Payroll Case Study; Significant tax fraud', 26 November 2019; and David Marin-Guzman, ''Architect' of Plutus tax fraud pleads guilty', *The Australian Financial Review,* 26 November 2019.
[30] David Marin-Guzman, 'Fourth Plutus tax fraud conspirator sentenced to jail', *The Australian Financial Review,* 10 July 2020.
[31] ATO, 'Plutus Payroll founder jailed in Operation Elbrus', 31 July 2020.
[32] Ibid.
[33] Cactus Consulting, 'Plutus Payroll Case Study; Significant tax fraud', 26 November 2019.

Geelong baker Barry Santoro allegedly had his identity stolen and was convicted of corporations offences for companies he did not know he was the director of. He was one of a number of people, including people who were homeless, who were allegedly used as straw directors to allow the real beneficial owners of the companies to cheat the tax office and other creditors of more than $100 million.[34] The alleged scheme involved stripping businesses of their cash and assets in order to cheat the tax office and other creditors, and then phoenixing under a different name. The straw directors were installed to shield the real directors from liquidators, creditors and ASIC.[35] In the same scheme, Christopher Somogyi, who had been homeless at the time, was fined more than $6 million through director penalty notices and other fines after his identity was allegedly used without his knowledge as a straw director for a number of companies.[36]

The Age reported in October 2020 of an Australian lawyer that advises clients to use Seychelles' private foundations to conceal the true ownership of companies and conceal activities from law enforcement agencies. He was quoted as advising "In the event of a lawsuit or tax investigation or regulatory inquiry, your client can swear under oath, 'I am not the legal or beneficial owner of this company', which could be the difference between being charged with/ jailed for tax evasion and walking away a free man."[37] People providing such fronts for potential criminal activity are not innocent third parties.

Criminals can also use the computers of innocent third parties as zombie bots in the criminal activity.[38] In March 2020, a network of nine million zombie bots being used for criminal activity was shut down.[39] In October 2020, it was reported in the media that Microsoft took legal action to try to shut down a zombie bot network of one million computers being hijacked for serious criminal activity.[40] The AFP shut down the use of the Imminent Monitor Remote Access Trojan in November 2019, which was being used to create zombie bots with the computers of Australians and others for serious criminal activities by a global network of criminals.[41]

22. Is the proposed additional threshold for group warrants appropriate?

The Synod supports that there be dedicated group warrants to target situations where a warrant in relation to individual members of the group would be impractical or ineffective. Effective law enforcement online 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.[42] Access to the data that shows interactions between people also allows police to identify those facilitating severe criminal activities, such as businesses providing

[34] Dan Oakes,' Bake made director of companies he'd never heard of in $100m tax scam, court hears', ABC News, 27 August 2018.
[35] Ibid.
[36] Ibid.
[37] Nick McKenzie, Charlotte Grieve and Joel Tozer, 'Lawyer who built a booming practice on finding loopholes', *The Age,* 20 October 2020.
[38] For background on the use of zombie bot networks for serious criminal activity see Kim-Kwang Raymond Choo, 'Zombies and botnets', Australian Institute of Criminology Trends and Issues No. 333, March 2007.
[39] 'Microsoft takes down global zombie bot network', BBC News, 11 March 2020, https://www.bbc.com/news/technology-51828781
[40] Frank Bajak, 'Microsoft attempts takedown of global criminal botnet', AP, 13 October 2020.
[41] Australian Federal Police, 'The Rat Trap: international cybercrime investigation shuts down insidious malware operation', 30 November 2019.
[42] Australian Criminal Intelligence Commission, 'Submission to the Parliamentary Joint Committee on Intelligence and Security Review of Mandatory Data Retention', July 2019, 3.

encrypted communication.[43] Such data can also help police locate victims[44], to rescue them from further harm.

An example of the need for such a warrant applies to networks of offenders involved in online child sexual abuse. Child sexual abuse perpetrators operate in networks online to assist each other.[45] 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.[46]

One site dedicated to hosting and distributing sexual abuse material involving infants and toddlers had over 18,000 registered members who regularly met online to discuss their preference for the sexual abuse of children in this age group.[47] A forum dedicated to discussing the abuse of children exceeded 23 million visits.[48]

One of the groups on Whatsapp that shared images and videos of children being sexually abused had 256 members.[49]

Operation Arkstone exposed one such network of child sexual abuse offenders. The joint operation between the Australian Federal Police, NSW Police, Queensland Police Service, WA Police and US Homeland Security Investigations rescued 46 Australian children from further abuse by November 2020.[50] The Australian Centre to Counter Child Exploitation received a report in February 2020 from the US National Centre for Missing and Exploited Children about an online user allegedly uploading child abuse material. That led to a 30-year old Wyong man being arrested in February 2020 and subsequently charged with 89 counts of child abuse. Investigation into the man's online activities led the AFP to social media forums where some members were allegedly producing child sexual abuse material, while others were accessing and circulating the material. As each member of the network was arrested, more offenders were discovered and more children rescued from further harm. The 14 Australian offenders in the network who were arrested came from many walks of life, from a childcare worker, volunteer soccer coach, disability support worker, an electrician, supermarket employee and chef.

Through the online forums used by the offenders uncovered by Operation Arkstone, a further 146 offenders were identified in Europe, Asia, the US, Canada and New Zealand and referrals were made to law enforcement agencies in those locations.

[43] Ibid., 3.
[44] Ibid., 4.
[45] 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.
[46] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 15.
[47] Ibid., 16.
[48] Ibid., 16.
[49] 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
[50] Australian Federal Police, 'Operation Arkstone results in 828 charges laid with 46 child victims identified', Media release, 11 November 2020.

The eSafety Commissioner publicly raised concerns in July 2021 that the chat app Kik allowed people to be completely anonymous[51], which facilitates networks involved in online child sexual absue. The app allows people identified only by a username to share photos and videos. It also allows them to video chat and find or form chat groups. Ramiz Adam was able to log into Kik using anonymous identities and share child sexual abuse material with more than 4,000 users. Kik stated on their website they would only comply with US judicial requests and only provide transaction chat logs. The company deletes all video and images after 30 days, destroying evidence of the sharing of child sexual abuse on its platform.[52]

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.[53]

Recent investigations have also 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.[54]

23. What are your views on the above proposed approach? Are there any other matters that should be considered by an issuing authority when considering necessity and proportionality?
The Synod supports the proposed factors outlined in the discussion paper for the test of necessity and proportionality in the use of electronic surveillance powers. The additional item the Synod recommends is the urgency with which the information is needed, such as the need to gather the information to prevent on-going child sexual abuse and rescue the child or children in question.

25. What are your thoughts on the proposed principles-based, tiered approach to use and disclosure?
The Synod supports the proposed principles-based, tiered approach to the use and disclosure of information. We would support information being disclosed and used for 'secondary purposes' applying to any information that relates to a criminal offence that carries at least a maximum penalty of four years in prison under Commonwealth or State and Territory laws. Such information should be shared with the law enforcement agency that has jurisdiction over the offence in question.

26. When should agencies be required to destroy information obtained under a warrant?
Agencies should be able to retain information for the duration of any investigation and subsequent judicial action. Once such needs have been met the information should be destroyed after three years. Our concern is that the information may be relevant for a

[51] Tessa Akerman, 'Paedophiles find prey in anonymous app', *The Australian,* 24 July 2021.
[52] Ibid.
[53] Canadian Centre for Child Protection, 'How we are failing children: Changing the paradigm', 2019, 20.
[54] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 14.

subsequent investigation into the same suspected offender or offenders, so a requirement for immediate destruction could compromise the effectiveness of a subsequent investigation.

27. What are your thoughts on the proposed approach to emergency authorisations?
The Synod supports that emergency authorisations be available to:

- Prevent or lessen imminent threats to life, or of serious harm or serious damage to property;
- Locate and investigate suspected kidnappings;
- Locate missing persons; and
- Recover a child subject to a child recovery order.

In addition to these factors, emergency authorisations should be permitted where there is a imminent danger evidence will be destroyed or where normal authorisation is likely to allow the suspected offender to evade the law enforcement agency.

US law enforcement agencies can act without a warrant in exigent circumstances. These are when:[55]

1. Evidence is in imminent danger of destruction;
2. A threat puts either the police or the public in danger;
3. The police are in "hot pursuit" of a suspect; or
4. The suspect is likely to flee before the officer can secure a search warrant.

In *United States v. Gorshkov*, 2001 WL 1024026, at *4 (W.D. Wash. 23 May 2001) law enforcement officers downloaded content, not just metadata, from a computer in Russia without a warrant. They were permitted to do so because probable cause existed to believe that the Russian computer contained evidence of crime and there was good reason to fear that delay could lead to destruction of or loss of access to evidence. The agent copied the data and subsequently obtained a search warrant.[56]

The Synod supports that the framework should take a technology-neutral approach to the way in which agencies can make applications.

29. Is there a need for statutory protections for legally privileged information (and possible other sensitive information, such as health information)?
While the Synod supports protection for legally privileged information, there is a need for some caution as some law firms may seek to claim legal privilege over a wide range of material to try and protect the criminal activities of their clients from investigation by law enforcement agencies. The Synod notes that the ATO has been forced to challenge excessive use of legal privilege seeking to frustrate its investigations into potential tax evasion and tax avoidance.

In March 2019, the Commissioner of Taxation expressed concern over the excessive use of claiming legal privilege:[57]

[55] US Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 2009, 27-28. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf
[56] Ibid., 29.
[57] Chris Jordan, 'Taxing times: positioning the ATO as an instrument of democracy', Address to the tax Institute 34th National Convention, Grand Chancellor Hotel, Hobart, 14 March 2019.

But when lawyers are claiming privilege on thousands or tens of thousands of documents – and we have seen this – we start to wonder if it's a genuine claim or an effect to conceal a contrived tax arrangement.

It all comes back to fairness- are you using legal professional privilege because you have a genuine need, or as a way to cheat the system? We'll be taking a tougher stance in the future?

The ATO has stated that dozens of audits of multinational corporations have been interrupted by claims of legal privilege. The ATO has warned that it would seek penalties and may take legal action against advisers who made "reckless or baseless LPP claims in an attempt to withhold facts and evidence from the Commissioner."[58]

In April 2020, the ATO launched legal action against Carlton United Breweries after the corporation tried to use legal privilege to withhold information during a tax audit. Justice Mark Moshinsky ruled in favour of the ATO in February 2021.[59]

The ATO has alleged in court in a case relating to JBS that PwC included a "relatively inexperienced lawyer" in tax advice to "apply a cloak of privilege" that would prevent regulators from being able to demand access to large companies' tax information.[60] The ATO is seeking access to approximately 44,000 documents related to JBs' tax affairs, with the ATO contesting the claims of legal privilege over 15,500 of them.[61]

It has been alleged that large accountancy firms have been misusing legal privilege to withhold tax and auditing information from regulators and shareholders.[62]

In addition to onshore firms that might assist in frustrating law enforcement investigations through the misuse of legal professional privilege, there are also offshore law firms that may also be willing to provide such a service.

The ATO was unsuccessfully challenged by Glencore that the ATO should not have been able to access copies of files relating to Glencore that had been leaked from Bermudian law firm Appleby through the Paradise Papers leak.[63]

Consideration needs to be given to prevent meritless claims of legal privilege being used to frustrate legitimate law enforcement investigations into serious human rights abuses and severe criminal activity. Creating a regime where it is easy to claim legal privilege over information could risk creating a business model for some law firms to effectively sell legal privilege as a shield against law enforcement agencies being able to access information, or at least impede such access.

---

[58] Hannah Wootton, 'PwC accused of misusing legal privilege to stop ATO scrutiny of clients', *The Australian Financial Review,* 7 September 2021.
[59] Charlotte Grieve, "Very uncomfortable position': ATO won't rule out criminal charges in PwC legal stoush', *The Sydney Morning Herald,* 3 February 2021.
[60] Hannah Wootton, 'PwC accused of misusing legal privilege to stop ATO scrutiny of clients', *The Australian Financial Review,* 7 September 2021.
[61] Ibid.
[62] Ibid.
[63] Nassim Khadem, 'ATO cracks down on legal professional privilege 'misuse' after Paradise Papers tax leak', *ABC News,* 14 March 2019.

30. What are the expectations of the public, including industry, in relation to oversight of these powers, and how can a new oversight framework be designed to meet those expectations?

The Synod expects that the oversight framework will ensure that law enforcement agencies only exercise the use of their powers in full compliance with the law. The use of such powers should be free from any political interference from the executive arm of government. There should be significant sanctions for law enforcement members that willfully misuse the powers entrusted to them.

33. Are there any additional reporting or record-keeping requirements agencies should have to improve transparency, accountability and oversight?

The Synod believes that law enforcement agencies and intelligence agencies should be required to report on how many warrants have been issued and in relation to which offences, so that the public are clear about what the frequency of use of these powers and which crimes they are being targeted at. There should also be annual reporting on how often metadata has been accessed and in relation to what offences. While such reporting will add to the administrative burden, it will provide transparency and accountability. It is builds on-going evidence about which powers are needed and for which crime types, so the public can be confident that the powers are needed and are being appropriately targeted.

37. Do you have views on how the framework could best implement the recommendations of these reviews? In particular:
c. Is it appropriate that the Public Interest Advocate framework be expanded only in relation to journalists and media organisations?

The Synod agrees that where a law enforcement agency investigation impacts on the legitimate professional activities of journalists and media organisations, the Public Interest Advocate framework may help provide protection of media outlets exposing corruption and maladministration. However, the evidence of what contribution it makes to the public interest is exceedingly limited.

The Public Interest Advocate framework should not apply when the journalist or media outlet are engaged in criminal activity not related to their professional functions. There have been rare cases of Australian journalists being involved in online child sexual abuse. For example, in September 2017, former Channel 9 journalist Ben McCormack pleaded guilty to charges relating to child sexual abuse material. He had traded explicit messages relating to child sexual abuse online. He had used the user name 'oz4skinboi' and during his online communication outlined his sexual interest in young boys.[64] In one exchange he claimed to have child sexual abuse videos and links to child sexual abuse images:[65]

> Male: … I have some vids… wbu?
> Ben McCormack: some
> Male: cool, cool, pics too?
> Ben McCormack: none saved but links

[64] Mazoe Ford and Antonette Collins, 'Ben McCormack, former A Current Affair reporter, pleads guilty over child porn charges', ABC news, 26 September 2017, https://www.abc.net.au/news/2017-09-26/ben-mccormack-a-current-affair-former-journalist-pleads-guilty/8987272
[65] Ibid.

Journalists and media outlets should not be entitled to any special consideration or protection when the law enforcement activity relates to criminal activity they have been suspected of being involved in. For media outlets, that should also include cases of tax evasion.

While extremely rare, the *News of the World* scandal demonstrates the need to ensure that media outlets are not permitted to be granted privileges that would give them a status that could hinder or frustrate an investigation into criminal activity they have been involved in, even when it relates to journalism. *News of the World* journalists illegally accessed voicemails of murdered schoolgirl Milly Dowler.[66] Thousands of people were targeted for phone hacking by *News of the World* journalists.[67] The practice of phone hacking was also in widespread use by journalists and staff at *The Mirror* and *Sunday People*, which continued to settle cases in 2021.[68]

Former *News of the World* editor Andy Coulson was convicted of conspiracy to hack phones.[69] One of its private investigators and the *News of the World*'s royal editor were imprisoned in 2007 over a story gleaned from phone hacking.[70] Private investigator Glenn Mulcaire, news editors James Weatherup and Greg Miskiw and journalists Neville Thurlbeck and Dan Evans pleaded guilty to conspiracy to hack phones.[71] The jury in the Coulson case was discharged after failing to reach verdicts on charges that Mr Coulson and Clive Goodman conspired to commit misconduct in a public office by bribing police officers for two royal directories.[72]

In his investigation into the culture, practices and ethics of the media in the UK in 2012, The Right Honourable Lord Justice Leveson came to the conclusion that: "There is no organised profession, trade or industry in which the serious failings of the few are overlooked because of the good work of the many."[73] We acknowledge that Justice Leveson was primarily referring to unethical conduct by a minority of journalists, rather than criminal activity. However, Justice Leveson pointed out that a private detective, Steve Whittamore, had been engaged in wholesale criminal breaches of data protection legislation. He argued that *prima facie,* journalists who engaged his services or used his products (and paid substantial sums for the privilege) must or should have appreciated that the information could not have been obtained lawfully.[74] Despite that, not a single journalist named in the Whittamore notebooks was ever interviewed, investigated or prosecuted for breaches of section 55 of the *UK Data Protection Act.*[75]

Justice Leveson's findings also offer a warning about creating special regimes for journalists and media outlets who may engage in criminal activity, including when that criminal activity relates to their journalistic activities. He pointed out that police investigations had been hindered and impeded by a lack of co-operation from News International and the law relating to search and seizure of journalistic material put many hurdles in the way of the police.[76] In relation to

[66] Jim Waterson, 'News of the World: 10 years since phone-hacking scandal brought down tabloid', *The Guardian,* 10 July 2021.
[67] Ibid.
[68] Ibid.
[69] BBC, 'Phone-hacking trial explained', 25 June 2014.
[70] Ibid.
[71] Ibid.
[72] Ibid.
[73] The Right Honourable Lord Justice Leveson, 'An Inquiry into the Culture, Practices and Ethics of the Press', Executive Summary, 29 November 2012, 5.
[74] Ibid., 7.
[75] Ibid., 23.
[76] Ibid., 13.

News of the World, he concluded that, "Suffice to say that in the absence of a complaint, luck, or, for the most serious crime, intelligence-led policing, possible offending of this type will not be detected."[77]

The Synod is supportive of more transparency around the existing Public Interest Advocate arrangements with annual public reporting on:

- The number and identity of Public Interest Advocates;
- The number of cases where a Public Interest Advocate contested a journalist warrant;
- The number of cases where a Public Interest Advocate attended the hearing of an application for a journalist warrant; and
- The number of journalist warrants that were successfully contested or modified as the result of the intervention by a Public Interest Advocate.

There is limited information on the value of the Public Interest Monitors in Victoria and Queensland. We have been unable to locate any independent assessment of the benefits of these roles in addressing warrants for surveillance activities.

In the *Victorian Public Interest Monitor Annual Report 2020-21*, the Victorian PIM reported on the number of relevant applications made by law enforcement agencies, the number in which the PIM appeared and the number that were refused. The PIM appeared in 45 of 250 Victoria Police applications, and 10 of 25 IBAC applications (and didn't appear in any other law enforcement agencies' applications). Six of the 250 Victoria Police applications were refused, and one of the 25 IBAC applications were refused. (There is no breakdown of how many of these the PIM appeared in.)

The Queensland *22nd Annual Report – Public Interest Monitor (2019-20)* reported that the PIM made submissions in all the warrant applications brought by the Queensland Police Service (QPS) and the Crime and Corruption Commission (CCC). The QPS made 56 applications for surveillance device warrants and all were granted (there is no information as to whether any were opposed by the PIM). Of the 19 warrant applications made by the CCC (18 surveillance device warrants; one cover search warrant), none was opposed by the PIM and all were granted.

Dr Mark Zirnsak
Senior Social Justice Advocate
Phone: +61-3-9340 8807
E-mail: mark.zirnsak@victas.uca.org.au

[77] Ibid., 13.