Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA

SUBMISSION TO THE SENATE LEGAL AND CONSTITUTIONAL AFFAIRS COMMITTEE
INQUIRY INTO *CRIMES LEGISLATION AMENDMENT (SEXUAL CRIMES AGAINST CHILDREN AND COMMUNITY PROTECTION MEASURES) BILL 2017*
29 September 2017

Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600

The Justice and International Mission Unit, Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes the opportunity to make a submission on the *Crimes Legislation Amendment (Sexual Crimes Against Children and Community Protection Measures) Bill 2017*. The Uniting Church in Australia has a strong commitment to protect children from child sexual abuse. The Unit will only comments on parts of the Bill where it has conducted research in the past.

The Unit strongly supports Schedule 2 – Use of video recordings to strengthen the protections of Part IAD of the *Crimes Act* for vulnerable witnesses (such as children) who give evidence in particular criminal proceedings, including for Commonwealth child sex offences and human trafficking and slavery offences. The Unit notes that the amendment to not have to seek leave to use a video recording of a vulnerable witness is an approach already adopted by States and Territories.

The Unit supports Schedule 3 to remove the requirement for vulnerable witnesses to be available to give evidence at committal proceedings. The Unit agrees that the amendment, by prohibiting cross-examination at committal proceedings or proceedings of a similar kind, means vulnerable witnesses will be spared an additional risk of re-traumatisation. As noted in the Explanatory Memorandum, it will bring the Commonwealth into line with practice in other Australian States and Territories.

The Unit supports Schedule 4 to introduce new aggravated offences that relate to child sexual abuse. While the Unit supports the increased penalties for these serious acts of harm against children, the Unit believes that greater impact in terms of deterrence is achieved through increasing the risk of detection and this is where more impact can be achieved. The risk of getting caught and the public shame that follows, with loss of relationships and employment in addition to any length of time in prison, is far more likely to deter many offenders than a the threat of a longer prison term if the would be offender believes their chance of getting caught is small.

To that end the Unit continues to urge the Commonwealth Government to fund research into Australian offenders who commit child sexual offences to identify their pathways to offending and assist in identifying measures to reduce this criminal activity.

The Unit supports the insertion of a new offence to criminalise using a postal or similar services to “groom” another person to make it easier to procure persons under 16 years of age for sexual activity. The Unit supports this offence having extra-territorial reach as is proposed in the Bill. The Unit notes the recent estimate from the US-based International

Centre for Missing & Exploited Children that there are 750,000 predators online at any given moment.[1] The International Centre for Missing & Exploited Children has assessed Australia's anti-grooming legislation as already amongst the best in the world.[2]

The International Centre for Missing & Exploited Children has recommended that cases where parents have been groomed to support the commission of the sexual abuse of the children in their care should be differentiated from those involving parents who are complicit in the grooming of their own child.[3]

The International Centre for Missing & Exploited Children has stated in relation to extra-territorial jurisdiction:[4]

> *Extraterritorial jurisdiction regarding the commission of sexual offenses against children is crucial. Extraterritorial jurisdiction offers a country a mechanism to hold its offenders accountable by providing the authority needed to prosecute its nationals for criminal acts committed beyond its borders. Dual criminality provisions, which require that a crime committed abroad must also be a crime in their home country, should be eliminated as they pose significant obstacles to the effectiveness of extraterritorial jurisdiction.*

The Unit supports the insertion of 'fictitious persons' in the *Criminal Code* in relation to grooming offences to allow for the use of standard investigatory techniques for this crime type, whereby a law enforcement agent assumes the identity of a fictitious person (whether a child or a third party) and interacts with potential offenders before they have an opportunity to sexually abuse a real child. Canada, Greece and New Zealand, among other countries, have updated their legislation to ensure that online undercover operations used to apprehend online offenders are admissible in court proceedings.[5] The International Centre for Missing & Exploited Children has similarly recommended that "Legislation must stipulate that a real child need not be involved to effectively prosecute offenders caught in such undercover operations."[6] Further they state:[7]

> …. *undercover operations can give law enforcement an advantage in the detection, prevention, and prosecution of child sexual abuse and exploitation, especially offenses involving online abuse. Covert online operations are a proactive method allowing investigators to pose as children and enter chatrooms and other online communities without needing to alter their physical identity or investing months in establishing a cover identity, as offline investigations require. In proactive operations, a crime has not yet been reported and law enforcement officers work to deter criminal offense before it occurs, as opposed to reactive operations after the commission of a crime….*
>
> *Specifically with regard to online grooming, in the absence of a meeting occurring between an offender and a victim, sexually exploitative interactions, via computer-*

[1] International Centre for Missing & Exploited Children, 'Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review', 1st Edition, 2017, p. 1.
[2] International Centre for Missing & Exploited Children, 'Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review', 1st Edition, 2017, p. 40.
[3] International Centre for Missing & Exploited Children, 'Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review', 1st Edition, 2017, p. 17.
[4] International Centre for Missing & Exploited Children, 'Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review', 1st Edition, 2017, p. 18.
[5] International Centre for Missing & Exploited Children, 'Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review', 1st Edition, 2017, p. 31.
[6] International Centre for Missing & Exploited Children, 'Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review', 1st Edition, 2017, p. 29.
[7] International Centre for Missing & Exploited Children, 'Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review', 1st Edition, 2017, pp. 29-30.

> *mediated communication, may only ever come to the attention of police authorities when a victim comes forward or discloses the abuse, or as a result of proactive undercover police operations. Thus online undercover operations help law enforcement to proactively identify offenders and possible offenders without waiting for child victims to come forward. Beyond detecting criminal activity, undercover operations can also aid prosecutions and deterrence by providing credible, direct (as opposed to circumstantial) evidence.*

Strike Force Trawlers and the NSW police reported nearly one arrest per week in 2016 and had eight arrests by April 2017 largely as a result of covert operations online. Those arrested ranged from teenagers to 70-year-olds, including teachers, fathers, priests and police academy students. While some cases involve a fictitious child, the majority of cases, nearly 70%, begin with a real child and a tip from parents who noticed a worrisome online conversation that they reported to police.[8]

The Unit supports the insertion of a new section 474.23A to criminalise the provision of an electronic service with the intention that the service will facilitate the commission of an offence against sections 474.22 (using a carriage service for child abuse material) or 474.23 (possessing, controlling, producing, supplying or obtaining child abuse material for use through a carriage service) of the *Criminal Code.* The UK Internet Watch Foundation reported that in 2016 they detected 57,335 webpages containing child sexual abuse imagery up from 13,182 webpages hosting child sexual abuse material in 2013.[9] There was also an increase in the number of individual images of children being hosted, with 293,818 images being viewed.[10] Trend data from the UK Internet Watch Foundation has shown the proportion of images of victims of child sexual abuse under the age of 10 has been decreasing in the last two years from 74% in 2011 to 81% in 2012 and 2013 to 69% in 2015 and 53% in 2016.[11] In 2016 2% of the images detected by the Internet Watch Foundation involved the sexual abuse of children aged two or under.[12] At the same time the proportion of images of child sexual abuse showing sexual activity between adults and children including rape and sexual torture decreased, as shown in Table 1.

Table 1. Proportion of images viewed by the Internet Watch Foundation showing penetrative sexual activity involving children including rape and sexual torture 2011 – 2016. [13]

Year	2011	2012	2013	2014	2015	2016
Proportion of images showing penetrative sexual activity with children	64%	53%	51%	43%	34%	28%

The Internet Watch Foundation reported detecting 455 newsgroups that hosted child sexual abuse material in 2016.[14]

[8] International Centre for Missing & Exploited Children, 'Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review', 1st Edition, 2017, p. 30.
[9] Internet Watch Foundation, 'IWF Annual Report 2016', p. 18; and Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', pp. 6, 17.
[10] Internet Watch Foundation, 'IWF Annual Report 2016', p. 6.
[11] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 11; Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', p. 6; Internet Watch Foundation, 'IWF Annual Report 2016', p. 9.
[12] Internet Watch Foundation, 'IWF Annual Report 2016', p. 9.
[13] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 11; Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', p. 6; and Internet Watch Foundation, 'IWF Annual Report 2016', p. 9.
[14] Internet Watch Foundation, 'IWF Annual Report 2016', p. 8.

The Internet Watch Foundation reported that in 2016 image hosts are most consistently abused for distributing child sexual abuse imagery. Offenders distributing child sexual abuse imagery commonly use image hosts to host the images which appear on their dedicated websites, which can often display many thousands of abusive images.[15]

In terms of online media hosting child sexual abuse images, in 2016 the Internet Watch Foundation reported 41,364 image hosts, 6,223 cyberlockers, 2,776 banner sites, 1,681 image boards, 826 blog sites, 803 online forums, 727 web archives, 643 social networking sites and 634 images stores.[16]

The Internet Watch Foundation also reported that in 2016 they have seen criminals increasingly using masking techniques to hide child sexual abuse images and videos on the internet and leaving clues to paedophiles so they can find it. Since 2011, the Internet Watch Foundation has been monitoring commercial child sexual abuse websites which only display child sexual abuse imagery when accessed by a "digital pathway" of links from other websites. When the pathway is not followed or the website is accessed directly through a browser, legal content is displayed. This means it's more difficult to find and investigate the illegal imagery They saw a 112% increase in this technique in 2016 over 2015, with 1,572 sites using this technique in 2016.[17]

The number of newly identified hidden services (on the 'dark web') detected by the Internet Watch Foundation declined from 79 in 2015 to 41 in 2016. They postulated that it is possible this could be the result of increased awareness by law enforcement internationally about hidden services distributing child sexual abuse imagery. Hidden services commonly contain hundreds or even thousands of links to child sexual abuse imagery that's hosted on image hosts and cyberlockers on the open web.[18]

Particularly problematic in failing to cooperate with law enforcement in removing child sexual abuse material online have been image hosts like Imager and TOR, including Depfile, which uses fastfluxing to change IP address rapidly in an effort to frustrate the efforts of law enforcement. The child sexual abuse site Playpen was established on TOR.[19]

The Financial Coalition Against Child Pornography has also reported criminal businesses that provide "bulletproof hosting" to defeat the system of take down notices against child sexual abuse material. These hosts promise customers their websites will not be taken down, regardless of complaints or content. Bulletproof hosts use a combination of distributed services to maintain uptime for their customers. Specific tactics they use include:[20]

- Registering the domain name with a registrar with relaxed enforcement. Depending on the location and enforcement policies, some registrars are used more heavily than others for illicit activities.
- Sharing and shuffling IP addresses to minimise downtime if particular IPs are shut down. This ensures content remains up while being indifferent to the status of particular domains. Instead of relying on one IP, bulletproof hosting relies on multiple IPs that can keep the content up independent of specific IP shut downs.

[15] Internet Watch Foundation, 'IWF Annual Report 2016', p.11.
[16] Internet Watch Foundation, 'IWF Annual Report 2016', p.11.
[17] Internet Watch Foundation, 'IWF Annual Report 2016', pp. 5, 17.
[18] Internet Watch Foundation, 'IWF Annual Report 2016', p. 13.
[19] 'Child abuse site creator jailed for 30 years', BBC News, 8 May 2017, http://www.bbc.com/news/technology-39844265
[20] Financial Coalition Against Child Pornography, 'Report on Trends in Online Crime and Their Potential Implications in the Fight Against Commercial Child Pornography', 1 February 2011, pp. 12-13.

- Using a standardised yet specific naming methodology for name servers to minimise service interruption.
- Soliciting business and communicating with customers using unmonitored, private media. Bulletproof hosts frequently advertise their services on message boards frequented by their target customer base. From there, e-mail, instant messaging and other non-public options are used to further business dealings. This allows bulletproof hosting services to remain largely underground and reduces exposure to enforcement entities.
- Collecting payment using unregulated payment services to limit scrutiny and preserve anonymity. The use of small payment processors originating from outside the US is popular due to lax regulatory environments and lessened cooperation with law enforcement agencies.

The hosting of child sexual abuse material online is the result of those in charge of the various online media either not being vigilant, through to having a reckless disregard for what is being hosted to deliberate facilitation. There is a need for the law to deal with those that intentionally facilitate distribution and hosting of child sexual abuse material and this Bill does address this problem. The Unit supports the extraterritorial jurisdiction that will be applied to this offence in the Bill.

The Unit supports the clarification of section 474.25A of the *Criminal Code* in the Bill of the scope of the conduct captured by the offence including live-streamed child abuse. The involvement of Australians as both producers and consumers of live-streamed child abuse on a commercial basis was noted by UNICEF in the Philippines as far back as 2005:[21]

> *In recent times, coinciding with the Internet boom, cybersex joints have opened. These are establishments that employ men, women and children to perform live sexual acts, which are then broadcast on the Internet via webcam. These sexual acts range from taking their clothes off to masturbating for the customers and doing other similar acts. It is also reported that there are cybersex joints where both heterosexual and homosexual acts are caught on webcam. Customers with Internet connections and credit cards may view these from a computer at home anywhere in the world.*
>
> *A number of these joints are found in Central Luzon. Lani (not her real name), who works full time for a local NGO, confirms the existence of numerous cybersex joints in their area. Most of these joints are operated by foreigners, mostly Australians and Americans, who have made the country their home. Usually, these foreigners have Filipino partners for their front men. She suspects that the owners of these joints have business partners abroad. Moreover, she also confirms that these cybersex joints employ children as young as 15 years old.*
>
> *The NBI [National Bureau of Investigation] also confirms that adult online entertainment providers exist in the country. These joints are offshore offices of adult online service providers in Western countries such as the United States. In May 2003, the NBI raided one of these joints, located at the plush San Lorenzo Village in Makati. According to the Inquirer (2003), the company was run by an American national. The joint's main office, however, is located somewhere in Nevada. It keeps an offshore office in the Philippines because it is much cheaper to operate here; Filipinas are paid much less than their US counterparts, and less money is spent on office maintenance. The company set up shop in a Makati mansion, which they subdivided into 10 different rooms, each room having two computers each complete with web cameras.*

[21] Arnie Trinidad, *Child Pornography in the Philippines,* Psychosocial Trauma and Human Rights Program UP Centre for Integrative and Development Studies and UNICEF Manila, 2005, pp. 48-49.

> *The company, according to a NBI agent interviewed for the report, employed more than 20 women who went on eight hour shifts, twenty four hours a day. Not surprisingly, the company also employed teenage children. In the raid, the NBI were able to rescue two children aged 16 and 17. The women and girls who worked for the company were not regular women in prostitution, as some were found to be college students while others were waitresses who were either recruited directly by the owners or by their friends.*

The Unit strongly supports the increased penalty in section 474.25 of the *Criminal Code* for Internet Service Providers and Internet Content Hosts who become aware that the service they provide can be used to access particular material that they have reasonable grounds to believe is child abuse material to have to refer the details of that material to the Australian Federal Police within a reasonable time. Ideally there should be an explicit requirement for ISPs and Internet Content Hosts to take all reasonable steps to assist law enforcement agencies to identify who is responsible for the child abuse material and who has accessed it, when requested to assist by law enforcement. There is currently no obligation under section 474.25 of the *Criminal Code* to report any clients accessing child sexual abuse material to the AFP.

By contrast Section 9 of the Philippines Republic Act No. 9775 *An Act Defining and Penalising the Crime of Child Pornography, Prescribing Penalties Therefor and for Other Purposes* has the following requirements:

- "All internet service providers (ISPs) shall notify the Philippines National Police (PNP) or the National Bureau of Investigation (NBI) within seven (7) days from obtaining facts and circumstances that any form of child pornography is being committed using its server or facility. Nothing in this section may be construed to require an ISP to engage in the monitoring of any user, subscriber or customer, or the content of any communication of any such person."
- "An ISP shall preserve such evidence for purposes of investigation and prosecution by relevant authorities."
- "An ISP shall upon the request of proper authorities, furnish the particulars of users who gained or attempted to gain access to an internet address which contains any form of child pornography."

Section 11 of the Filipino law requires internet content hosts to "Within seven (7) days, report the presence of any form of child pornography, as well as the particulars of the person maintaining, hosting, distributing or in any manner contributing to such internet address, to the proper authorities."

Also, under US criminal law §2258A of USC Title 18 provides that any ISP that becomes aware of its servers being used to provide child pornography material must report that to national authority (the Cyber Tipline). ISPs must furnish as soon as possible a report that includes various information in relation to the identifying material of individuals who it is aware of that are registered as controlling the material. It also requires that ISPs provide the details of any other customers of theirs who access the material in the period prior to the material being taken down. Liability for breaching any of the rules of §2258A is set at a company level (in the form of fines), but individual directors or officers of companies cannot be criminally prosecuted unless it can be shown that they acted intentionally or recklessly.

The Unit supports the amendment to paragraph 16A(2)(g) of the *Crimes Act 1914* that an offender be offered a reduction in their sentence for an early guilty plea as it saves victims and witnesses from the often harrowing experience of giving evidence and being cross-examined in open court.

The Unit supports the proposed paragraph 16A(2)(ma) to the *Crimes Act 1914* that introduces as a new consideration whether the person's standing in the community was used to aid in the commission of the offence, as a factor in aggravating the seriousness of the criminal behaviour to which the offence relates.

The Unit supports the new subsection 16A(2AAA) to the *Crimes Act 1914* which will require a court to have regard to the objective of rehabilitation of the offender when determining the sentence to be passed or order to be made.

The Unit strongly supports the repeal of all references in the *Criminal Code* and throughout Commonwealth legislation of 'child pornography material' and replacing these references with a single definition of 'child abuse material'. The use of 'child abuse material' reflects the terminology used by those who work with survivors of child sexual abuse and law enforcement. 'Child pornography' still appears in some international conventions and in early laws written to criminalise the material. Given the growing acceptance of pornography as a legitimate product in Western societies, the term 'child pornography' is now seen to offer some legitimacy to the material in question when it should be regarded as unacceptable and criminal. The term is also used by opponents of the full range of measures needed to eliminate such material. The AFP have for years provided advice to media at the bottom of media releases related to offences committed in relation child sexual abuse material stating:

Note to media: CHILD EXPLOITATION IMAGES, NOT 'CHILD PORNOGRAPHY'
Use of the phrase 'child pornography' actually benefits child sex abusers:

- *It indicates legitimacy and compliance on the part of the victim and therefore legality on the part of the abuser*
- *It conjures up images of children posing in provocative positions, rather than suffering horrific abuse*
- *Every photograph captures an actual situation where a child has been abused. This is not pornography.*

It would make sense for Commonwealth legislation to reflect the advice of the law enforcement agency with the responsibility of combating the production, distribution and consumption of child sexual abuse material.

In addition to the measures in the Bill the Unit repeats its request from 2012 that the Commonwealth Government implement the recommendation of the UN Committee on the Rights of the Child from 19 June 2012 to develop and implement a comprehensive and systematic mechanism of data collection, analysis, monitoring and impact assessment of child sexual abuse offences. This should include data collected on the number of prosecutions and convictions, disaggregated by the nature of the offence.

Dr Mark Zirnsak
Director
Justice and International Mission Unit
Synod of Victoria and Tasmania
Uniting Church in Australia
130 Little Collins Street
Melbourne Victoria 3000