Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA

E-mail: [redacted]

Submission from the Uniting Church in Australia, Synod of Victoria and Tasmania to the *Assistance and Access Bill 2018*

10 September 2018

The Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes the opportunity to make a submission on the *Assistance and Access Bill 2018*. The Uniting Church in Australia has a strong commitment to protect children from child sexual abuse. To that end, and to combat other serious criminal activity, the Synod supports the *Assistance and Access Bill 2018.*

The Synod supports the things specified in notices issued under the Bill must be for the purpose of assisting a law enforcement agency perform its core functions conferred under law, as they specifically relate to:

- Enforcing the criminal law and laws imposing pecuniary penalties, or
- Assisting the enforcement of the criminal laws in force in a foreign jurisdiction, or
- Protecting the public revenue.

The Synod has some hesitancy about 'safeguarding national security' being one of the objectives of the notices, as it is not clear what additional activities this captures that are not criminal activities. For example, notices to address terrorist activities are already about enforcing criminal laws as would be notices targeting foreign espionage. We have a concern that 'safeguarding national security' might mean the desire of a government of the day to target civil society groups and individuals that oppose its policies or to target whistleblowers that expose wrong-doing by the government of the day. It would be good if the explanatory memorandum of the Bill includes an explanation of what non-criminal activities are intended to be caught under 'safeguarding national security' under the Bill.

The Bill appears to strike the right balance between giving law enforcement agencies the increased powers they need to protect vulnerable members of the community from serious harm by those engaged in serious criminal activity that involves electronic communication while providing safeguards against misuse and over-reach.

The Synod notes that unauthorised disclosure of information obtained under the powers of the Bill can result in a law enforcement agent being sent to prison for up to ten years, while a controller of a technology corporation or senior employee of such a corporation that wilfully obstructs a criminal investigation will not face imprisonment.

The need for ICT corporations being required to assist law enforcement by force of law is being increasingly recognised globally. For example, the International Centre for Missing and Exploited Children found 79 governments out of 196 now had laws requiring ISPs to retain digital user data to ensure access to data for the purposes of prosecuting child sexual exploitation offences.[1]

The Synod is aware there are ICT corporations that have an ideological position that privacy of their clients is paramount, and thus can be reckless in designing services that frustrate

[1] International Centre for Missing and Exploited Children, 'Child Pornography: Model Legislation and Global Review', 8th Edition, 2016, p.vi.

efforts of law enforcement to stop child sexual abuse, terrorism and other serious criminal activity. Government needs to ensure law enforcement has the power and tools to address such reckless behaviour by those ICT corporations that otherwise act to frustrate the legitimate and necessary activities of law enforcement.

For example, Simon Hackett the managing director of Internode in 2011 appeared to publicly state that his company would only assist law enforcement combat serious criminal activity to the extent that the law requires them to do so:[2]

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

Further:[3]

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

Multinational ICT corporations have also acted to frustrate the efforts of law enforcement. For example, Brian Lee Davis in the US confessed to owning hundreds of digital photos and videos that showed young children being raped. In July 2017 he was sentenced to a decade in a state prison. Law enforcement sought to pursue the entire child exploitation network he had been part of. State investigators were unable to access emails that could have helped them identify victimized children and track down the offenders Mr Davis admitted to contacting. Although Google tipped off law enforcement about the child exploitation files that had crossed its network, the corporation refused to give them access to his gmail account, despite the fact that police had a search warrant.[4]

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

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

The company eventually won before the federal appellate court in New York on 14 July 2016. The ruling said the *Stored Communications Act* does not give American judges "extraterritorial" powers, and that therefore they cannot grant search warrants that reach outside the United States. A US judge could not demand that a company give up a video held on a European machine, for instance, even if it documented a crime committed by one American against another on American soil.[5]

Since the legal decision, major technology corporations such as Microsoft and Yahoo defied judges' orders in criminal investigations, refusing to turn over potentially crucial digital

[2] https://delimiter.com.au/2011/12/28/post-iinet-internode-maintains-cautious-filter-stance/
[3] https://delimiter.com.au/2011/07/05/well-filter-when-the-law-makes-us-internode/
[4] https://money.cnn.com/2017/10/19/technology/criminal-investigations-microsoft-ireland-invs/index html
[5] https://money.cnn.com/2017/10/19/technology/criminal-investigations-microsoft-ireland-invs/index html

evidence of crimes. Their actions impeded hundreds of criminal investigations, according to public testimony to Congress and interviews with law enforcement officials by CNN.[6] These cases include ones of human trafficking, drug smuggling, and fraud.

Thus if the legislation only required co-operation where it was already possible to decrypt communication, this would send a signal to some ICT corporations to ensure they develop technology that cannot be readily decrypted, to thwart any requirement to co-operate with law enforcement agencies.

While it is appropriate that the Bill carries civil penalties, injunctions and enforceable undertakings for designated communication providers that refuse to co-operate with law enforcement agencies under a technical assistance notice or technical capability notice, a review should also be conducted after three years to see if these sanctions have been sufficient to ensure co-operation. If these sanctions have proved to be inadequate, criminal penalties should apply to those inside the providers that wilfully refuse to assist law enforcement agencies when the law requires them to do so. The Synod notes that such penalties will apply under Schedules 3 and 4 of the Bill for a refusal to comply with an enhanced search warrant.

Online child exploitation remains a serious global problem in which thousands of Australia participate in accessing, sharing and trading in child exploitation material. The UK Internet Watch Foundation reported that in 2017 they detected 78,589 urls containing child sexual abuse imagery up from 13,182 urls hosting child sexual abuse material in 2013.[7] There was also an increase in the number of individual images of children being hosted, with 293,818 images being viewed.[8] 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 from 74% in 2011 to 81% in 2012 and 2013 to 69% in 2015 to 53% in 2016 and 55% in 2017.[9] In 2016 and 2017 2% of the images detected by the Internet Watch Foundation involved the sexual abuse of children aged two or under.[10] 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 – 2017. [11]

Year	2011	2012	2013	2014	2015	2016	2017
Proportion of images showing penetrative sexual activity with children	64%	53%	51%	43%	34%	28%	33%

[6] https://money.cnn.com/2017/10/19/technology/criminal-investigations-microsoft-ireland-invs/index html
[7]Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', p. 15; and Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', pp. 6, 17.
[8] Internet Watch Foundation, 'IWF Annual Report 2016', p. 6.
[9] 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; Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', p. 6.
[10] Internet Watch Foundation, 'IWF Annual Report 2016', p. 9 and Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', 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; and Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', p. 16.

The Internet Watch Foundation reported detecting 571 newsgroups that hosted child sexual abuse material in 2017 compared to 455 in 2016.[12]

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.[13]

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.[14]

The Internet Watch Foundation also reported that in 2016 and 2017 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.[15] This increased again in 2017, with 2,909 websites using this method to hide child sexual abuse material.[16]

The number of newly identified hidden services (on the 'dark web') detected by the Internet Watch Foundation declined from 79 in 2015 to 41 in 2016 and then increased to 44 in 2017. They postulated that 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.[17]

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.[18]

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.

Given the global nature of online child exploitation and the need for law enforcement agencies to co-operate across borders, the Synod strongly supports the amendments to the *Mutual Assistance in Criminal Matters Act 1987* contained in the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* to ensure that where

[12] Internet Watch Foundation, 'IWF Annual Report 2016', p. 8; and Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', p. 15.
[13] Internet Watch Foundation, 'IWF Annual Report 2016', p.11.
[14] Internet Watch Foundation, 'IWF Annual Report 2016', p.11.
[15] Internet Watch Foundation, 'IWF Annual Report 2016', pp. 5, 17.
[16] Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', p. 24.
[17] Internet Watch Foundation, 'IWF Annual Report 2016', p. 13 and Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', p. 20.
[18] 'Child abuse site creator jailed for 30 years', BBC News, 8 May 2017, http://www.bbc.com/news/technology-39844265

information is obtained in response to a computer access warrant for a domestic investigation, the Attorney General may authorise the provision of that information to a foreign government in response to a mutual assistance request. However, the restrictions under Part IIIBB that the offence being investigated must carry a penalty of at least three years or more imprisonment under the law of the foreign jurisdiction could result in some cases where the foreign law enforcement agency cannot be assisted in investigating online child exploitation. The International Centre for Missing and Exploited Children reported in their 2016 assessment of 196 jurisdictions, 35 jurisdictions have no legislation at all to address online child exploitation and 50 governments have not criminalised the knowing possession of online child sexual exploitation material.[19]

Thus, in some jurisdictions accessing online child exploitation material may carry less than a three year imprisonment as the maximum penalty. A foreign law enforcement agency might be investigating a ring of people accessing child sexual abuse material and sharing such material in which Australian citizens are participating. The foreign law enforcement agency may which to learn more about the network through knowing what the Australians accessing the network are doing. However, in this case the co-operation might not be able to proceed if the Australians in question would face less than three years imprisonment for their activities under the laws of the foreign jurisdiction. It would be better if the Bill were amended so that co-operation can be provided if the offences in question carry a maximum penalty of three years imprisonment or more under the laws of the foreign jurisdiction or under Australian law.

The Synod does not support Australian law enforcement agencies providing assistance where the offence carries the death penalty in the foreign jurisdiction.

The Synod supports the amendments to allow the Attorney-General to authorise applications to computer access warrants under the *Surveillance Devices Act 2004* when a request is received from the International Criminal Court or a Tribunal established under the *International War Crimes Tribunal Act 1995*.

Dr Mark Zirnsak
Director
Justice and International Mission Unit
Synod of Victoria and Tasmania
Uniting Church in Australia
[redacted]
Phone: [redacted]
E-mail: [redacted]

[19] International Centre for Missing and Exploited Children, 'Child Pornography: Model Legislation and Global Review', 8th Edition, 2016, p.vi.