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

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

Submission by the Synod of Victoria and Tasmania, Uniting Church in Australia to the inquiry into the mandatory data retention regime prescribed by Part 5-1A of the *Telecommunications (Interception and Access) Act 1979*
1 July 2019

The Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes this opportunity to make a submission to the mandatory data retention regime prescribed by Part 5-1A of the *Telecommunications (Interception and Access) Act 1979*. The Unit is supportive of metadata retention, as a vital instrument in the fight against online child sexual abuse. The Australian Federal Police have identified the vital role metadata retention plays in the being able to identify and prosecute offenders engaged in online child sexual abuse. The failure to maintain mandatory data retention will undoubtedly assist large numbers of offenders escape detection and prosecution each year, reducing the effectiveness of the Australian Federal Police in combating this crime type and other serious harms to people. It will be certain where technology corporations are not required to retain data, they will destroy the data to gain a cost saving through both not having to pay the storage costs and through not having to assist law enforcement as they will no longer have to provide evidence of serious criminal activity involving the harm of people as they will have been able to destroy it. It has been amply demonstrated that many technology corporations will almost always put their profits ahead of the well-being of the community.

There must not be any reduction in the length data needs to be retained, if anything it should be extended. Where an Australian paedophile has engaged in hundreds of sessions of live rape, torture and sexual abuse of children via webcam over a number of years, a court should not be hampered in its sentencing determination by the fact that a profit-driven technology corporation has wiped the evidence of sessions because of an inadequate data retention period exists.

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.

The Synod takes the view that when encountering evidence of serious criminal activity, the people running any business would report the evidence of the criminal activity to law enforcement agencies and absorb the cost of doing so. For example, if a rental car business found evidence of blood stains in one of their vehicles suggesting it had been used in a violent crime, the Synod would expect that the people running the business would report the evidence

and preserve it, not clean the car and destroy the evidence. Or if a train company recorded the rape of a child on their service through CCTV then the Synod would expect that the people running the train business would voluntarily hand over the footage and assist in identifying the rapist to police. The Synod would not expect the staff in the train business to seek to uphold the privacy rights of the rapist and hinder the police investigation by wiping the CCTV footage. Unfortunately, the people running multinational technology businesses often appear to fail to live up to this standard, even resisting assisting police when court orders have been issued.

Table of Contents

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

1. Uniting Church position on curbing sexual abuse

The Uniting Church in Australia nationally has had a strong focus on responding to cases of child sexual abuse within the Uniting Church's own operations.

At the same time, the clearest statement opposing all sexual abuse was made by the 1991 Assembly meeting:

> *91.18.1/2 The Assembly resolved:*
> *To receive the report (of the Commission for Women and Men)*
> *(a) That sexual violence be deplored as a sin against God and humanity.*
> *(b) That it be recognized that the origin of sexual violence lies in the practice of inequality of the sexes;*
> *(c) That it be confessed that sexual violence is disturbingly frequent within the Uniting Church community as it is in the wider community;*
> *(d) That it be acknowledged that in the past, the church has often made inappropriate responses or no response to victims/survivors of sexual violence. This has been experienced by many as a further violation;*
> *(e) That the church be committed to hearing the voices of those who are victims of sexual violence;*
> *(f) That the actions of people who work for the end of such violence and who support its victims/survivors be supported;*
> *(g) That the urgent need for the church community to become part of a "network of prevention" in the area of sexual violence be recognized;*
> *(h) That the publication "The Pastoral Report to the Churches on Sexual Violence Against Women and Children of the Church Community" be commended to presbyteries and parishes as a guide for study and action.*

This resolution committed the Uniting Church to hearing the voices of survivors of sexual abuse and to be part of wider efforts to prevent sexual violence.

There is an explicit statement opposing child sexual abuse from the Uniting Church National Assembly Standing Committee meeting of March 2013 (ASC Minute 13.07.03):

> *The sexual abuse of children is criminal behaviour that is totally abhorrent and unacceptable.*

The Uniting Church in Australia National Assembly has issued a Uniting Church values statement in relation to the Royal Commission into Child Sexual Abuse:[1]

> *The Uniting Church believes that God has given us the gift of the Spirit to "constantly correct that which is erroneous" in our life (Basis of Union, Para 18). Therefore, we will not hide from the truth, however painful that may be, and we will seek, with compassion and humility, to address whatever issues and challenges may emerge for us. We will say "sorry" to anyone who was sexually abused when in our care and, in consultation with those so affected, actively seek for ways to make amends for what happened in the past and identify how we can best offer support into the future. In all of this we are guided by the Word of God, remembering the teaching of the Apostle Paul: "Whatever is true, whatever is honourable, whatever is just, whatever is pure, whatever is pleasing, whatever is commendable... think about these things" (Philippians 4:8).*

[1] https://assembly.uca.org.au/rcvalues

From the beginning of our life together as the people of God within the Uniting Church in Australia, we have sought through prayer, and a spirit of consensus, to discern what it means to confess Jesus as Lord and Head over all things (Basis of Union, Para 3). At the time of Inauguration, the Assembly spoke to the nation in a statement that has guided and encouraged us ever since to be a church that honours Christ in all that we say and do. The statement declared, in part, that "we affirm our eagerness to uphold basic Christian values and principles, such as the importance of every human being, the need for integrity in public life, and the proclamation of truth and justice... We pledge ourselves to seek the correction of injustices wherever they occur" (Statement to the Nation, National Assembly, June 1977).

To adopt such a stance in the life of our nation means that we must be willing to examine our own motives and behaviour and be open to accept the close scrutiny of others. In that regard the Uniting Church welcomes the decision of the Federal Government to establish a Royal Commission on the sexual abuse of children in both public and church institutions, and pledges itself to cooperate fully and honestly with the process the Commission will implement. The sexual abuse of children is criminal behaviour that is totally abhorrent and unacceptable.

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

93.4.3.5 The Synod resolved:
That the Victorian Government be requested to provide for the protection of women and children from rape, domestic violence and incest by:
(i) Developing and maintaining long term programs of preventative community education.
(ii) Requiring the Department of Public Prosecutions to provide information and advice to victims.
(iii) Collecting and publishing accurate information concerning sex crimes.
(iv) Enhancing education for police officers, in particular for the officers of the Uniform and Community Policing Unit, so that they better understand and can better implement codes of practice for sexual assault victims.
(v) Increasing support for victims of sexual assault by resourcing programs specializing in offering services to victims.
(vi) Encouraging and resourcing research and education designed to assist judges in sentencing, particularly sentencing involving crimes of sexual assault.

The second is from 1994 calling on the Victorian Government to take a holistic response to child sexual abuse in the community:

94.2.4.1 The Synod resolved:
(a) That the Synod call on the Victorian Government to provide additional funding for preventative services to assist children "at risk" of child abuse.
(b) That the Synod request the Victorian government to develop a "holistic" strategy to respond to child abuse which ensures that once reports are investigated that families receive long term support.
(c) That the Synod encourage Ministers and Parish leaders to attend the "Strengthening Vulnerable Families" day and/or use the resources developed.

The third is from 2011 and explicitly addresses online child sexual abuse, calling on the Federal Government to adopt measures to deter online child sexual abuse, increase its detection and resource police to address all cases where Australians are involved in online child sexual abuse:

11.6.18.2.4 The Synod resolved:

(a) *To call on the Federal Government to adequately resource the Australian Federal Police to investigate all cases of online child sexual abuse where either the perpetrator or the victim is Australian;*

(b) *To call on the Federal Government to require Internet Service Providers (ISPs) to take action to assist in combating the sale, transmission and accessing of child sexual abuse images, which are always produced through human trafficking, forced labour, slavery or other means of manipulation and coercion. To that end the Federal Government is requested :*

- *To leave the IT industry in no doubt that they have a legal obligation to report clients accessing child sexual abuse material when they detect it, regardless of privacy legislation; and*
- *To legislate to require ISPs to block client access to all websites that contain material classified as 'Refused Classification', regardless of where such sites are hosted, and to log attempts by clients to access child sexual abuse sites and provide this information to the authorities for investigation;*

(c) *To call on the Federal Government to urge those countries that have not yet criminalised the production, distribution, use and possession of child sexual abuse material to do so; and*

(d) *To write to the Prime Minister, the Minister for Home Affairs, the Minister for Broadband, Communications and the Digital Economy, the Leader of the Opposition, the Shadow Minister for Home Affairs, the Shadow Minister for Broadband, Communications and the Digital Economy, and the Leader of the Greens to inform them of this resolution.*

In this resolution the Synod resolved that technology corporations should be required to report all cases of their clients accessing child sexual abuse material.

2. Child Sexual Abuse Online

We completely agree with former Prime Minister Tony Abbott that, "As a community we must have zero tolerance for the sexual abuse of children. Wherever abuse has occurred it must be tackled and it must be tackled vigorously, openly and transparently."[2]

Police around the world face a substantial challenge in stopping people being involved in child sexual abuse offences. This involves everything from grooming children for actual physical offences to the production of and trading in images of child sexual abuse. The commercial trade in images of child sexual abuse involves hundreds of sites. An estimated 50,000 new child sexual abuse images are produced each year.[3] The industry is estimated to be worth about US$250 million globally.[4]

In 2018 the Australian Federal Police received approximately 18,000 reports of child sexual abuse material being accessed by Australians. This includes a growing number of cases where Australians connect with human traffickers in the Philippines via social media to arrange for the live streaming of a child being sexually abused. In these cases a web camera located in the Philippines is used to stream live video of a child being subjected to sexual abuse with the Australian giving real time instructions on what abuse should be carried out. Hundreds of Australians have been detected involved in this abuse, with any single Australian paedophile paying for hundreds or thousands of sessions of abuse over the course of a number of years. A single session of child sexual abuse can cost as little as $20.

The eSafety Office assisted in the facilitation of the take-down of more than 5,000 child sexual abuse items hosted overseas in the 2016-2017 financial year and more than 8,000 such items in the 2017-2018 financial year.[5]

Research and the experience of law enforcement officials is that people engaged in the rape, torture and sexual abuse of children of all ages and who trade in images, videos or stream such horrific activity are adaptive and respond to both the opportunities new technologies provide as well as adapt to law enforcement strategies. It tends to be the least intelligent and least adaptive perpetrators that will be easiest for law enforcement to apprehend.

Online child sexual exploitation remains a serious global problem in which thousands of Australia participate in accessing, sharing and trading in child sexual 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.[6] There was also an increase in the number of individual images of children being hosted, with 293,818 images being viewed.[7] In 2018 the Internet Watch Foundation removed 105,047 webpages

[2] The Hon Tony Abbott MHR, Media Release, "The sexual abuse of children", 12 November 2012.
[3] UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010
[4] ibid.
[5] Lynelle Briggs, 'Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the *Broadcasting Services Act 1992* (Online Content Scheme), October 2018, 11.
[6] 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.
[7] Internet Watch Foundation, 'IWF Annual Report 2016', p. 6.

showing sexual abuse and sexual torture of children.[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, as shown in Table 1.

Table 1. Proportion of images viewed by the Internet Watch Foundation showing victims of child sexual abuse under the age of 10.[9]

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

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] In 2018 the Internet Watch Foundation reported that it viewed 1,300 images of the sexual abuse of infants and babies.[11] 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 2.

Table 2. Proportion of images viewed by the Internet Watch Foundation showing penetrative sexual activity involving children including rape and sexual torture 2011 – 2017. [12]

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

The Internet Watch Foundation reported detecting 571 newsgroups that hosted child sexual abuse material in 2017 compared to 455 in 2016.[13]

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

[8] Internet Watch Foundation, 'Record number of images showing children being sexually abused removed by UK internet charity', 23 January 2019.
[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.
[9] Internet Watch Foundation, 'IWF Annual Report 2016', p. 9; Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', p. 6 and Internet Watch Foundation, 'Record number of images showing children being sexually abused removed by UK internet charity', 23 January 2019.
[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, 'Record number of images showing children being sexually abused removed by UK internet charity', 23 January 2019.
[12] 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.
[13] Internet Watch Foundation, 'IWF Annual Report 2016', p. 8; and Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', p. 15.

commonly use image hosts to host the images which appear on their dedicated websites, which can often display many thousands of abusive images.[14]

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.[15]

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.[16] This increased again in 2017, with 2,909 websites using this method to hide child sexual abuse material.[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 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.[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.

[14] Internet Watch Foundation, 'IWF Annual Report 2016', p.11.
[15] Internet Watch Foundation, 'IWF Annual Report 2016', p.11.
[16] Internet Watch Foundation, 'IWF Annual Report 2016', pp. 5, 17.
[17] Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', p. 24.
[18] Internet Watch Foundation, 'IWF Annual Report 2016', p. 13 and Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', p. 20.

3. The need for data retention in the fight against online child sexual abuse

The Australian Federal Police has stated data retention is crucial to being able to fight a range of serious criminal activity, including online child sexual abuse offences. This need was noted in research by the Australian Institute of Criminology in 2009:[19]

> *The modern criminal, using the same devices as today's teenagers, communicates with Voice over Internet Protocol, video instant messaging, cellular camera phone, and text messaging in computer slang that is foreign to most police officers and parents. The trail to uncover this valuable investigation resource often starts with a forensic examination, but this trail quickly grows cold as Internet Service Providers overwrite logs and data retention periods expire. All police agencies are facing the same challenge when dealing with computer forensics. Police managers must find a way to examine an increasing number of digital devices, each containing an immense volume of data, in a timely manner and with limited resources.*

The Asia-Pacific Financial Coalition Against Child Sexual Exploitation issued a guidance paper to file hosting and file sharing companies in September 2013, *Confronting New Challenges in the Fight Against Child Pornography: Best Practices to Help File Hosting and File Sharing Companies Fight the Distribution of Child sexual Exploitation Content*, which stated:[20]

> *Both for Internet Service Providers and file sharing companies, data retention and preservation are critical functions in the fight against child pornography. File sharing companies should strongly consider logging IP's and discouraging/preventing a customer's use of proxies to log onto a company's URL.*

The Synod is aware that globally child sexual abuse offenders have sometimes managed to escape being brought to justice because ISPs and other communications companies have wiped the data vital to the police being able to make a case. The Australian Federal Police stated that it wa facing the problem that Australian ISPs and communication companies were also wiping data records more quickly prior to the introduction of the mandatory data retention regime, which will undermine investigations into serious offences. *The Australian* reported on 1 November 2014 that the Australian Federal Police stated that ISPs and communication companies were discarding data within weeks.[21] In one case, police had been able to track down 307 suspects allegedly involved in online child sexual abuse, but 156 escaped because of missing records of their activity.[22] The Commissioner of the Australian Federal Police, Andrew Colvin, also stated at a joint press conference on 30 October 2014:[23]

---

[19] Kim-Kwang Raymond Choo, 'Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences' Australian Institute of Criminology Research and Public Policy Series 103, 2009, p.82.

[20] Asia Pacific Financial Coalition Against Child Pornography, 'Confronting New Challenges in the Fight Against Child Pornography: Best Practices to Help File Hosting and File Sharing Companies Fight the Distribution of Child sexual Exploitation Content', September 2013, p. 4.

[21] Brendan Nicholson, 'Culprits are on the loose because of missing phone data, police say', *The Australian,* 1 November 2014, http://www.theaustralian.com.au/national-affairs/defence/culprits-are-on-the-loose-because-of-missing-phone-data-police-say/story-e6frg8yo-1227108941266

[22] Malcolm Turnbull, 'Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014', 30 October 2014, http://www.malcolmturnbull.com.au/media/speech-telecommunications-interception-and-access-amendment-data-retention; and Matthew Knott, 'Malcolm Turnbull introduces

> *If I could just give you a couple of examples of some child protection matters. I'll be reasonably generic but you'll understand the gist of the matter. A recent EUROPOL matter that identified 371 potential suspects for child abuse material in the UK, of that 371 IP addresses if you like, because the UK have solid data retention laws UK authorities were able to identify 240 individual suspects in that matter of which they prosecuted 120. Contrast that with another major, leading European country, quite sophisticated and developed in the way that it does business, the same investigation, a very similar number of IP addresses were identified in that country; 350 odd. They were only able to identify seven and didn't prosecute anybody because there are no data retention laws in that country and the data wasn't able to be made available.*

Further he stated:

> *So this is a real, pressing issue for law enforcement around the country at the moment, it is a matter that we deal with each and every day, not just in child protection operations, in serious and organized crime investigations, in our national security work, our physical assault, sexual assault, murders metadata is that fundamental tool that we use. It's the tool that we use often to place people at the scene of a crime, or remove them from suspicion. It's the tool that we use to help us refine what further intrusive matters or powers we may need to use down the track. As I say I can't underscore enough how fundamental it is.*

As noted in the previous inquiry by the Committee, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (p. 140):

> *Currently, authorised access to telecommunications data, such as subscriber details, generated by carriers for their own business purposes is an important source of information for agencies. As carrier's business models move to customer billing based on data volumes rather than communication events (for example number of phone calls made), the need to retain transactional data is diminishing. Some carriers have already ceased retaining such data for their business purposes and it is no longer available to agencies for their investigations.*

Further, the previous report provided an example (p. 166) of an alleged offender who had engaged in on-line sharing of child sexual abuse material whose identity and precise location could not be identified as the carrier was unable to provide the information despite the alleged criminal activity having occurred less than 24 hours prior.

The Synod is concerned by the arguments raised by some submissions in the *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* that people engage in serious harm to others online should not be required to make greater efforts to conceal their activities as a result of the Australian Government having in place mandatory data retention (pp.175-182). These arguments are regularly raised by those who oppose effective law enforcement online, and similar arguments have been raised by those opposed to disruption

---

legislation for metadata retention scheme', *The Sydney Morning Herald,* 30 October 2014, http://www.smh.com.au/federal-politics/political-news/malcolm-turnbull-introduces-legislation-for-metadata-retention-scheme-20141030-11e101.html#ixzz3Hf3OYMHb

[23] Senator, The Hon George Brandis QC, The Hon Malcolm Turnbull MP, Mr Duncan Lewis, Director-General of Security and Mr Andrew Colvin, Commissioner of the Australian Federal Police, Joint Press Conference, 30 October 2014.

tools of access to online child sexual abuse material or of the regulation of online currencies to reduce their use in money laundering. The argument is deeply flawed. While any improvement in tools for law enforcement to combat online criminal activity is likely to see some offenders adapt and use more sophisticated tools to avoid detection and capture, experience of law enforcement agencies is that many offenders do not adapt their behaviour and are more likely to get caught. The fact that many offenders engaged in extreme forms of online criminal activity do not currently make use of all the online tools available to them that would assist them in avoiding detection and capture is evidence that not all offenders have the knowledge or simply do not behave in a way that maximizes their ability to get away with their online criminal behaviour.

For example, offenders who access child sexual abuse material do not appear as sophisticated as is often assumed. The UNODC commented only 17% of offenders in a particular sample used password protection, 3% evidence – eliminating software and only 2% used remote storage systems.[24] They noted more sophisticated offenders could have evaded detection. However, such statistics serve as a warning that simply because a counter-strategy is technologically available does not mean all offenders will avail themselves of the strategy.

On this point the Virtual Global Taskforce stated in 2012:[25]

> *Levels of forensic awareness exhibited by offenders appear to interact with the environments used for CAM [Child Abuse Material] distribution and to be affected by the investigative priorities of law enforcement units. Accordingly, teams that focus on the more sophisticated offenders tend to encounter higher levels of forensic awareness, while those working primarily on public P2P [peer to peer] distribution may see very little. At the same time, identification in the recent VGT P2P study of a higher level of computer literacy amongst offenders with the deepest levels of involvement in online CSE [Child Sexual Exploitation] (based on a range, length and management of offending, and size of collection) may reflect an increase in technical skill in line with experience in offending, or indeed the extent to which the sophistication of a particular environment for offending may dictate the level of technical skill required for access, even preventing some offenders gaining access to new or more extreme material.*
>
> *The majority of offenders in the experience of respondents were identified as exhibiting either "some" or "good" forensic awareness, categories aligned with some form of password protection, IP masking, or evidence elimination. Other security measures cited include hard drive partitioning and physical secretion of portable hard drives and thumb drives, for instance behind false panels.*
>
> *As the above discussion on distribution methods indicates, however, the security consciousness of an individual offender can be shaped by a number of factors, including the default settings or preferred platforms, previous encounters with law enforcement, considerations of ease of access to CAM when desired, and the influence of other members of a particular online network. As one respondent noted, awareness is not the same as execution. Very few offenders are 100% secure all of the time or in all respects.*

[24] UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010.
[25] Virtual Global Taskforce, 'Virtual Global Taskforce Environmental Scan 2012', pp. 16-17.

> *The collecting impulse and sexual drive of offenders often prevents them from being as secure as they would like.*
>
> *Equally, offenders cannot entirely control the behaviour of others. Participating in online forums, while necessary to access newer material, was deemed by some respondents to be something of a risk in itself, even in those environments in which administrators enforce security standards. In this respect, anonymity is never absolutely assured.*

The argument put forward by those opposed to data retention would appear to be that because some offenders may adapt their behaviour in response to the maintenance of law enforcement capability and escape capture, then the capacity of law enforcement should be permitted to be eroded.

In contrast to those who make arguments about the development of online tools to assist offenders in escaping detection and capture, the UN Commission on Crime Prevention and Criminal Justice noted the on-going development of tools to detect serious criminal activity within large volumes of data, pointing to the value in retaining metadata. If the data is wiped, these data mining tools become useless in detecting online criminal activity. The UN Commission on Crime Prevention and Criminal Justice reported:[26]

> *The massive amount of data on the Internet can be used to assist in the prevention, detection, and prosecution of child exploitation crimes. In this context, data mining and analytics have undergone tremendous advancements in recent years…. In particular, social networking companies may be able to identify the kinds of profiles that most commonly trigger contact by offenders, and to undertake preventative or educational measures, or to share information with law enforcement authorities in response to requests made through due legal process.*
>
> *Data mining and analytics companies often work to continuously improve their software's ability to assemble relevant information in a law enforcement context. One large data analytics company, for example, worked with a child abduction resource centre to link an attempted abduction to previous hotline reports displaying similar traits. In a matter of minutes, the software had linked the relevant data from various databases and plotted the information on a map, which the investigative team could use to locate the suspect more quickly.*

The Synod notes concerns raised in the media that access to metadata is particularly important to ASIC "because communications are central to the most serious breaches of the corporations and securities law it polices, including insider trading, market manipulation and fraud. In the case of insider trading, communication is in effect the offence, and must be proved."[27] It was reported that the chairman of ASIC, Greg Medcraft, told the National Press Club in December 2014 that access to metadata was critical to investigate insider trading and market manipulation,

[26] UN Commission on Crime Prevention and Criminal Justice, 'Study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children', E/CN.15/2014/1, 7 May 2014, p. 46.
[27] Malcolm Maiden, 'ASIC gutted by metadata regime and fighting to hold ground', *The Age,* 13 November 2014.

as well as superannuation fraud.[28] He is reported to have stated to the media about the need for ASIC to have access to metadata without a warrant:[29]

> *At the end of the day we are a law enforcement agency and access to that data is critical to use in terms of clearly, insider trading, because that's how we can actually investigate people who have been involved in insider trading, and also market manipulation.*

Some online technology corporations and their management argue they will only assist police to the extent that they are forced to do so by the law. For example, Simon Hackett, the managing director of Internode in 2011, appeared to publicly state that his company would only assist police to combat serious criminal activity to the extent that the law requires them to do so:[30]

> *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:[31]

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

Facebook's policy on retaining evidence of criminal activity on its platform seems reasonable:[32]

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

However, unless Australian law continues to compel companies to retain metadata for two years, it would appear Facebook would cut this to one even when they know the data in question relates to the criminal harm of people. Further, despite being part of the same multinational corporation, Whatsapp does not make clear how long they will preserve data related to the serious harm of others for criminal investigation for.[33]

The Financial Times reported that videos and images of children being sexually abused were being openly shared on Facebook's WhatsApp on a vast scale.[34] Israeli researchers warned Whatsapp that it was easy to find and join dozens of chat groups where people were sharing images and videos of children being sexually abuses. In one case, one of these groups had 256 members.

---

[28] Gareth Hutchens and Georgia Wilkins, ' Metadata access simply crucial to ASIC enforcement', *The Age,* 4 December 2014.
[29] Clancy Yeats, 'ASIC calls for data to fight cyber crime', *The Age,* 27 November 2014.
[30] https://delimiter.com.au/2011/12/28/post-iinet-internode-maintains-cautious-filter-stance/
[31] https://delimiter.com.au/2011/07/05/well-filter-when-the-law-makes-us-internode/
[32] https://www.facebook.com/about/privacy
[33] https://www.whatsapp.com/legal/#privacy-policy-law-and-protection
[34] 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

By further contrast, Google makes it less clear they will preserve and report actionable child sexual abuse material and evidence of other serious criminal activity involving the harm of people in all cases:[35]

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

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

The 2018 documentary, 'The Cleaners'[36], has exposed how technology companies are exploiting people in the Philippines to screen social media and remove abusive material, including child sexual abuse material. These people reported they are expected to look at up to 25,000 images a day and get inadequate psychological support for being exposed to images of the worst depravity human beings are capable of. They also reported destroying the online evidence of child sexual abuse without referring it to police, destroying vital evidence that could assist police in rescuing children from on-going abuse.

It has been reported that the UK Parliamentary Intelligence and Security Committee has publicly expressed concern that even when ICT corporations detect terrorist material that poses a threat to the well-being of the community and would allow early detection of potential threats, they do not report the material to law enforcement agencies[37] (which is consistent with the evidence presented in the documentary '*The Cleaners'*).

[35] https://www.google.com/+/policy/content.html
[36] https://vimeo.com/ondemand/thecleaners2018
[37] UK Intelligence and Security Committee of Parliament, 'The 2017 Attacks: What needs to change?', 22 November 2018, 29.

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

4. Human Rights Obligations

The role of the Internet and other new technologies in facilitating more readily human rights abuses and transnational criminal activity has been receiving growing recognition globally. For example, the resolution of the UN Human Rights Council A/HRC/8/L.17 of 12 June 2008 called for governments:

> *2(g) To establish mechanisms, where appropriate, in cooperation with the international community, to combat the use of the Internet to facilitate trafficking in persons and crimes related to sexual or other forms of exploitation and to strengthen international cooperation to investigate and prosecute trafficking facilitated by the use of the Internet.*

The right to freedom of speech and expression outlined in the *International Covenant on Civil and Political Rights* includes the limitation that:

> *3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as provided by law and are necessary;*
> *(a) For respect of the rights or reputations of others;*
> *(b) For the protection of national security or of public order (ordre public), or of public health and morals.*

The UN Commission on Crime Prevention and Criminal Justice, in discussing the balance between States' obligations to combat child sexual exploitation and uphold the right to freedom of expression, has noted that:[38]

> *The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, identifies four forms of expression that are required to be prohibited by international law; child pornography; direct and public incitement to commit genocide; advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence; and incitement to terrorism.*

The Synod believes it is clear the number of Australians engaged in online child sexual abuse activities far outweighs the resources of law enforcement agencies to deal with them all. This combined with the egregious nature of child sexual abuse more than justifies data retention, as outlined in the Act, of all Australians for at least two years to maintain the capability of law enforcement to combat online child sexual abuse to the extent that their resourcing allows for. The demonstrated likelihood that without data retention hundreds, if not thousands, of offenders engaged in online child sexual abuse offences will escape detection and prosecution over time, should outweigh any concerns about the impact of data retention on the right to privacy.

It should also be remembered that the Australian Government has an obligation to uphold the human rights of victims of child sexual abuse online, a point that opponents of data retention usually neglect to mention. These rights include Article 7 of the *International Covenant on Civil and Political Rights:*

> *No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment.*

This right is violated for victims of online child sexual abuse.

[38] UN Commission on Crime Prevention and Criminal Justice, 'Study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children', E/CN.15/2014/1, 7 May 2014, p. 54.

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

Article 8 of the *International Covenant on Civil and Political Rights* states

> *2. No one shall be held in servitude.*
> *3. (a) No one shall be required to perform forced or compulsory labour;*

Victims of commercial child sexual abuse online, be it through the sale of live webcam abuse or through videos and images, have usually been subjected to servitude and forced labour. Australia has an obligation to take all reasonable steps to reduce demand from Australians of online child sexual abuse material, and effective law enforcement is one measure that is necessary towards achieving this goal. Data retention is a part of what is necessary for effective law enforcement.

The right to privacy itself, Article 17 of the *International Covenant on Civil and Political Rights,* states:

1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
2. *Everyone has the right to the protection of the law against such interference or attacks.*

Victims of online child sexual abuse have had their rights to privacy violated and have had their honour and reputations subjected to unlawful attacks. Thus, failure to act effectively to combat online child sexual abuse, is a failure to uphold the rights of victims of online child sexual abuse. In the view of the Synod, the obvious violations of the rights outlined in Article 17 of victims of online child sexual abuse outweigh any claimed violations of the privacy rights of Australians under Article 17 that would be supposedly caused by the data retention requirements of Part 5-1A of the *Telecommunications (Interception and Access) Act 1979*. It needs to be stressed that for the vast majority of Australians, law enforcement will never access the data retained under the requirements of the *Telecommunications (Interception and Access) Act 1979*, so there is no impact on the privacy of the vast majority of people whose data is not accessed.

Further, under the *Convention on the Rights of the Child,* to which Australia is a States Party, Article 16 states:

1. *No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.*
2. *The child has the right to protection of the law against such interference or attacks.*

Again, being the victim of online child sexual abuse is an unlawful attack on a child's honour, to which governments should take all reasonable steps to prevent. More explicitly Articles 34 to 36 require states to protect children from all forms of sexual exploitation and sexual abuse. Article 34 requires:

> *States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent:*
> *(a) The inducement or coercion of a child to engage in any unlawful sexual activity;*
> *(b) The exploitative use of children in prostitution or other unlawful sexual practices;*
> *(c) The exploitative use of children in pornographic performances and materials.*

Data retention, as outlined in Part 5-1A of the *Telecommunications (Interception and Access) Act 1979*, is a necessary step, in the opinion of the Synod, towards the Australian Government effectively fulfilling its obligations under Article 34.

The Australian Government also has obligations to effectively combat online child sexual abuse under the provisions of the *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.* Of particular relevance is Article 9, which states:

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

5. Assessment on Law Enforcement Agencies Use of Metadata

The Synod notes the assessment of the Commonwealth Ombudsman that:[39]

> *As a result of our 2016-17 inspections we formed the view that agencies were generally exercising their powers to access stored communications and telecommunications data appropriately. Agencies had frameworks in place to ensure appropriate access to intrusive powers and these frameworks appeared to be working as intended. Agencies also demonstrated a commitment to compliance and responded appropriately to compliance issues.*

The Commonwealth Ombudsman did report non-compliance in a relatively small number of cases in relation to:[40]

- Two cases relating to journalist information warrants;
- 12 breaches of required considerations;
- Four cases of telecommunication data accessed without proper authority;
- 39 cases of telecommunications data being outside the parameters of the authority;
- Two cases of the authorization not being in writing;
- 12 cases of non-compliance with written records indicating notification of an authorization;
- 11 cases of non-compliance with record keeping requirements; and
- Seven cases of transposing errors.

The most significant number of non-compliance cases was generated by the Australian Federal Police as a result of all authorisations of access to telecommunications data between 13 and 26 October 2015 made by ACT Policing were made by an officer not authorized under s 5AB(1A) of the Act. This issue resulted in 116 non-compliant authorisations during the period. This also meant there was a large number of non-compliant authorisations dating back to March 2015. The AFP advised the non-compliance occurred due to the Commissioner's written authorization under s 5AB(1A) failing to authorize any officers within ACT policing. The AFP advised this omission on the written authorization was due to an administrative oversight. Upon identifying the error, the AFP updated the Commissioner's written authorization on 26 October 2015 to appoint the relevant position within ACT Policing as an authorized officer.[41]

---

[39] Commonwealth Ombudsman, 'A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunication data under Chapters 3 and 4 of the *Telecommunications (Interception and Access) Act 1979* for the period 1 July 2016 to 30 June 2017', November 2018, 1.

[40] Commonwealth Ombudsman, 'A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunication data under Chapters 3 and 4 of the *Telecommunications (Interception and Access) Act 1979* for the period 1 July 2016 to 30 June 2017', November 2018, 7.

[41] Commonwealth Ombudsman, 'A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunication data under Chapters 3 and 4 of the *Telecommunications (Interception and Access) Act 1979* for the period 1 July 2016 to 30 June 2017', November 2018, 10.

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

Given the Commonwealth Ombudsman reported that all agencies were receptive to the findings, recommendations and suggestions of the Ombudsman, the Committee should wait for the next assessment by the Ombudsman before concluding any additional oversight or restriction is needed on agencies access to metadata. Should non-compliance rates not have reduced, then further measures of enhanced oversight should be considered by the Government.

None of the cases of cases of non-compliance by the Commonwealth Ombudsman resulted in serious harm to people, in contrast to cases where destruction of metadata will result in an increase of cases where children are subjected to rape, torture and other forms of sexual abuse due to law enforcement agencies being unable to identify perpetrators and victims without the relevant metadata being available.