Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA

E-mail: tech@humanrights.gov.au

Submission from the Uniting Church in Australia, Synod of Victoria and Tasmania to the Human Rights and Technology Issues Paper of the Australian Human Rights Commission

2 October 2018

The Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes the opportunity to make a submission in response to the *Human Rights and Technology Issues Paper.* As the paper acknowledges, new technology often can be used to both further people's human rights or to facilitate human rights abuses. This is usually not the result of the technology itself, but how it is used and how it is regulated.

The Synod has had a long standing involvement in addressing online child sexual abuse and is a member of the Asia Pacific Financial Coalition Against Child Pornography.[1]

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.[2] There was also an increase in the number of individual images of children being hosted, with 293,818 images being viewed.[3] 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.[4] In 2016 and 2017 2% of the images detected by the Internet Watch Foundation involved the sexual abuse of children aged two or under.[5] 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. [6]

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

[1] https://www.icmec.org/apac-fcacp/

[2] 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.

[3] Internet Watch Foundation, 'IWF Annual Report 2016', p. 6.

[4] 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.

[5] Internet Watch Foundation, 'IWF Annual Report 2016', p. 9 and Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', p. 6.

[6] 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 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 laws to deal with those that intentionally facilitate distribution and hosting of child sexual abuse material.

Online child sexual exploitation is a global problem and requires international co-operation to tackle it. 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.[7]

1. **What types of technology raise particular human rights concerns? Which human rights are particularly implicated?**

Our main concerns are with technologies that grant secrecy, which we find can be used to commit human rights abuses and escape being identified. We have dealt with cases where this secrecy has facilitated online child sexual abuse, the exploitation of workers who do not know who their real employer has been and in assisting human rights abusers to shift profits obtained from their abuses across borders to stash them from law enforcement agencies.

The Internet Watch Foundation 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 them. 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.[8] This increased again in 2017, with 2,909 websites using this method to hide child sexual abuse material.[9]

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.[10]

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.[11]

[7] International Centre for Missing and Exploited Children, 'Child Pornography: Model Legislation and Global Review', 8th Edition, 2016, p.vi.
[8] Internet Watch Foundation, 'IWF Annual Report 2016', pp. 5, 17.
[9] Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', p. 24.
[10] Internet Watch Foundation, 'IWF Annual Report 2016', p. 13 and Internet Watch Foundation 'Internet Watch Foundation Annual Report 2017', p. 20.
[11] 'Child abuse site creator jailed for 30 years', BBC News, 8 May 2017, http://www.bbc.com/news/technology-39844265

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 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:[15]

- 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.
- 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.

Being able to register companies online without adequate identification of the real owners and controllers of the company can create vehicles through which human rights abuses can be carried out with protection from being identified by law enforcement agencies. Research by Findley, Nielson and Sharman found Australian corporate service providers were near the top of corporate service providers in terms of being willing to set up an untraceable shell

[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] 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.

company even when there was significant risk the company in question would be used for illicit purposes.[16]

For example, AUSeCorporate[17] that advertise to foreign investors and business people providing a nominee service to conceal their ownership from public scrutiny.

As an example of a case where shell companies with concealed ownership were allegedly used to facilitate money laundering through Australia largely from human rights abuses, US authorities sought to seize the assets in three Westpac accounts held by Technocash Ltd holding up to $36.9 million.[18] Technocash Limited was an Australian registered company. The funds are alleged to be connected to shell companies owned by the defendants in the case connected to a criminal financial entity, Liberty Reserve.[19] According to the case filled by the US Attorney for the Southern District of New York, Liberty Reserve SA operated one of the world's most widely used digital currencies. Through its website, the Costa Rican company provided its with what it described as "instant, real-time currency for international commerce", which could be used to "send and receive payments from anyone, anywhere on the globe". The US authorities allege that people behind Liberty Reserve:[20]

> *…intentionally created, structured, and operated Liberty Reserve as a criminal business venture, one designed to help criminals conduct illegal transactions and launder the proceeds of their crimes. Liberty Reserve was designed to attract and maintain a customer base of criminals by, among other things, enabling users to conduct anonymous and untraceable financial transactions.*
>
> *Liberty Reserve emerged as one of the principal means by which cyber-criminals around the world distributed, stored and laundered the proceeds of their illegal activity. Indeed, Liberty Reserve became a financial hub of the cyber-crime world, facilitating a broad range of online criminal activity, including credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking. Virtually all of Liberty Reserve's business derived from suspected criminal activity.*
>
> *The scope of Liberty Reserve's criminal operations was staggering. Estimated to have had more than one million users worldwide, with more than 200,000 users in the United States, Liberty Reserve processed more than 12 million financial transactions annually, with a combined value of more than $1.4 billion. Overall, from 2006 to May 2013, Liberty Reserve processed an estimated 55 million separate financial transactions and is believed to have laundered more than $6 billion in criminal proceeds.*

It was further alleged by US authorities that for an additional "privacy fee" of 75 cents per transaction, a user could hide their own Liberty Reserve account number when transferring funds, effectively making the transfer completely untraceable, even within Liberty Reserve's already opaque system.[21]

---

[16] Michael Findley, Daniel Nielson and Jason Sharman, 'Global Shell Games: Testing Money Launderers' and Terrorist Financiers' Access to Shell Companies', Centre for Governance and Public Policy, Griffith University, 2012, p. 21.

[17] http://www.ausecorporate.com.au/corporate-services/australian-branch-subsidiary-company/

[18] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 29, 43.

[19] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 21.

[20] US Attorney for the Southern District of New York, 13 Civ 3565, 28 May 2013, pp. 4-5.

[21] US Attorney for the Southern District of New York, 13 Civ 3565, 28 May 2013, p. 6.

US authorities alleged defendant Arthur Budovsky used Technocash to receive funds from exchangers. Mr Budovsky, the alleged principal founder of Liberty Reserve,[22] allegedly used his bank to wire funds to Technocash bank accounts held by Westpac.[23] He is also alleged to be the registered agent for Webdata Inc which held an account with SunTrust. Technocash records allegedly showed deposits into the SunTrust account from Technocash accounts associated with Liberty Reserve between April 2010 and November 2012 of more than $300,000.[24]

Arthur Budovsky was allegedly listed as the president for Worldwide E-commerce Business Sociedad Anonima (WEBSA) and defendant Maxim Chukharev as the secretary. Maxim Chukharev was alleged to have helped design and maintain Liberty Reserve's technological infrastructure.[25] WEBSA allegedly served to provide information technology support services to Liberty Reserve and to serve as a vehicle for distributing Liberty Reserve profits to Liberty Reserve principals and employees.[26] It is alleged bank records showed that from July 2010 to January 2013, the WEBSA account in Costa Rica received more than $590,000 from accounts at Technocash associated with Liberty Reserve.[27]

It is alleged Arthur Budovsky was the president of Grupo Lulu Limitada which was allegedly used to transfer and disguise Liberty Reserve Funds.[28] Records from Technocash allegedly indicate that from August 2011 to November 2011 a Costa Rican bank account held by Grupo Lulu received more than $83,000 from accounts at Technocash associated with Liberty Reserve.[29]

Further, defendant Azzeddine El Amine, manager of Liberty Reserve's financial accounts,[30] was the Technocash account holder for Swiftexchanger. It is alleged e-mails showed that exchangers wishing to purchase Liberty Reserve currency wired funds to Swiftexchanger. When Swiftexchanger received funds in its Technocash account, an e-mail alert was sent to El Amine, notifying him of the transfer. Based on these alerts, it is alleged between 12 June 2012 and 1 May 2013, exchangers doing business with Liberty Reserve send approximately $36,919,884 to accounts held by Technocash at Westpac.[31]

The defendants are alleged to have used Technocash services to transfer funds to nine Liberty Reserve controlled accounts in Cyprus.[32]

Technocash Limited is reported to have been forced out of business in Australia following the action by US authorities, when it was denied the ability to establish accounts in Australia by

---

[22] US Department of Justice, 'One of the World's Largest Digital Currency Companies and Seven of Its Principals and Employees Charged in Manhattan Federal Court and Running Alleged $6 Billion Money Laundering Scheme', 28 May 2013.
[23] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 29.
[24] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[25] US Department of Justice, 'One of the World's Largest Digital Currency Companies and Seven of Its Principals and Employees Charged in Manhattan Federal Court and Running Alleged $6 Billion Money Laundering Scheme', 28 May 2013.
[26] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 37.
[27] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[27] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 38.
[28] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[28] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 40.
[29] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 36.
[29] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 41.
[30] US Department of Justice, 'One of the World's Largest Digital Currency Companies and Seven of Its Principals and Employees Charged in Manhattan Federal Court and Running Alleged $6 Billion Money Laundering Scheme', 28 May 2013.
[31] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 30.
[32] USA vs Liberty Reserve, US District Court, Southern District of New York, 13 CRIM368, para 31.

financial institutions.[33] Technocash stated that it "complied with Australia's comprehensive AML regime, verified customers and has an AFSL licence since 2003. Technocash denied any wrong doing."[34]

The Liberty Reserve case is also an example of how digital and virtual currencies can be used to facilitate human rights abuses, such as the purchase of child sexual abuse material, due to the lower level of regulation over digital and virtual currencies. However, this is starting to shift, with jurisdictions such as Australia requiring the providers of digital currencies to have to take steps to know their customers, in the same way that financial institutions are required to do to address the risks of money laundering and financing of terrorism.

3. **How should Australian law protect human rights in the development, use and application of new technologies? In particular:**
   (a) What gaps, if any, are there in this area of Australian law?
   (b) What can we learn about the need for regulating new technologies, and the options for doing so, from international human rights law and the experiences of other countries?
   (c) What principles should guide regulation in this area?

There is a need for law to address technologies that allow people to conceal their identities, when use of the technology could result in serious human rights violations. If a person believes that they can carry out human rights abuses with impunity (because they cannot be identified or traced), then more people will carry out such human rights abuses.

There need to be laws to address technology corporations, their owners and their employees that recklessly or intentionally facilitate human rights abuses or obstruct law enforcement agencies seeking to investigate human rights abuses.

Privacy and secrecy are two sides of the same coin. Protecting the privacy rights of people is important to protect them from abuses like identity theft. At the same time, the right to privacy must not include the right to conceal your identity in order to carry out human rights abuses or serious criminal activity. There is a need to balance these rights, granting appropriate protection to the legitimate privacy of people while allowing law enforcement agencies the tools they need to identify and seek prosecution of human rights abusers and criminals.

4. **In addition to legislation, how should the Australian Government, the private sector and others protect and promote human rights in the development of new technology?**

Technology companies should be willing to assist law enforcement agencies and regulators in identifying and investigating those involved in human rights abuses that are using the technology provided by the company where it is reasonable to do so. In our experience too many Australian technology companies see assisting law enforcement agencies in addressing human rights abuses as an unnecessary and burdensome cost, and often champion the privacy rights of clients over assisting law enforcement investigate human rights abuses. Of course the upholding of the privacy rights of clients also aligns with maximisation of profits for the companies in question.

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:[35]

[33] Technocash, 'Opportunity: Own the Technocash Payment Platform', Media Release, 5 July 2013.
[34] http://www.technocash.com/pages/press-release.cfm
[35] https://delimiter.com.au/2011/12/28/post-iinet-internode-maintains-cautious-filter-stance/

> *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:[36]

> *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.[37]

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.[38]

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 evidence of crimes. Their actions impeded hundreds of criminal investigations, according to public testimony to Congress and interviews with law enforcement officials by CNN.[39] These cases include ones of human trafficking, drug smuggling, and fraud.

Thus in March 2018 Congress passed the *Clarifying Overseas Use of Data Act* which allows law enforcement agents to demand that technology companies provide user data regardless of where the company stores the data. The Act formalizes the process for companies to challenge a law enforcement request. The Act imposes certain limits and restrictions on law

[36] https://delimiter.com.au/2011/07/05/well-filter-when-the-law-makes-us-internode/
[37] https://money.cnn.com/2017/10/19/technology/criminal-investigations-microsoft-ireland-invs/index.html
[38] https://money.cnn.com/2017/10/19/technology/criminal-investigations-microsoft-ireland-invs/index.html
[39] https://money.cnn.com/2017/10/19/technology/criminal-investigations-microsoft-ireland-invs/index.html

enforcement requests to address privacy and civil liberty concerns. The Act regulates access to the content of electronic communications and cloud-stored documents, as well as non-content data relating to electronic communications (like transmission records and user-account information), but not other types of personal or business data.

A provider may move to modify or quash a request for data from law enforcement if it "reasonably believes":

- that the "customer or subscriber is not a US person and does not reside in the US," and
- that disclosure would "create a material risk that the provider would violate the laws" of the foreign government.

A court can then modify or quash a law enforcement request to a provider if it finds that:

- disclosure would cause the provider to violate the laws of the foreign government;
- granting the challenge would serve "the interests of justice"; and
- the customer or subscriber is not a US person and does not reside in the US.

And for purposes of determining what "the interests of justice" require, the Act establishes specific factors for the court to consider, including: (i) the interests of the US and foreign government, (ii) the likelihood and nature of the penalties that would be imposed, (iii) the person and provider's connections to the US, or (iv) the importance of the information to the investigation, and the availability of other means to obtain the information.

Additionally, the Act allows providers to inform the foreign government of the law-enforcement request so that the foreign government can object directly to the U.S. government if it wishes.

6. How should Australian law protect human rights in respect of AI-informed decision making? In particular:

(a) What should be the overarching objectives of regulation in this area?

(b) What principles should be applied to achieve these objectives?

(c) Are there any gaps in how Australian law deals with this area? If so, what are they?

(d) What can we learn from how other countries are seeking to protect human rights in this area?

The Australian Government should introduce legislation to ban the production, sale, possession and use of fully autonomous weapon systems. Over the past decade, the expanded use of unmanned armed vehicles has dramatically changed warfare, bringing new humanitarian and legal challenges. Now rapid advances in technology are resulting in efforts to develop fully autonomous weapons. These robotic weapons would be able to choose and fire on targets on their own, without any human intervention. This capability would pose a fundamental challenge to the protection of civilians and to compliance with international human rights and humanitarian law.

Several nations with high-tech militaries, particularly the United States, China, Israel, South Korea, Russia, and the United Kingdom are moving toward systems that would give greater combat autonomy to machines. If one or more chooses to deploy fully autonomous weapons, a large step beyond remote-controlled armed drones, others may feel compelled to abandon policies of restraint, leading to a robotic arms race. Agreement is needed now to establish controls on these weapons before investments, technological momentum, and new military doctrine make it difficult to change course.

Allowing life or death decisions to be made by machines crosses a fundamental moral line. Autonomous robots would lack human judgment and the ability to understand context. These qualities are necessary to make complex ethical choices on a dynamic battlefield, to distinguish adequately between soldiers and civilians, and to evaluate the proportionality of

an attack. As a result, fully autonomous weapons would not meet the requirements of the laws of war.

The use of fully autonomous weapons would create an accountability gap as there is no clarity on who would be legally responsible for a robot's actions: the commander, programmer, manufacturer, or robot itself? Without accountability, these parties would have less incentive to ensure robots did not endanger civilians and victims would be left unsatisfied that someone was punished for the harm they experienced.

Dr Mark Zirnsak
Director
Justice and International Mission Unit
Synod of Victoria and Tasmania
Uniting Church in Australia