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

Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600
E-mail: legcon.sen@aph.gov.au

Submission by the Synod of Victoria and Tasmania, Uniting Church in Australia to the inquiry into the *Social Media (Anti-Trolling) Bill 2022*
28 February 2022

The Synod of Victoria and Tasmania, Uniting Church in Australia, welcomes this opportunity to make a submission to the inquiry on the *Social Media (Anti-Trolling) Bill 2022*. The Synod supports the Bill and believes it should be passed by the Parliament as it will create a very positive outcome of incentivising social media corporations to take steps to know who the natural people are behind online identities.

The Synod is deeply concerned about serious human rights abuses that occur online or are facilitated online, including child exploitation. Anonymous online identities help facilitate many of these serious human rights abuses, as outlined in the details below.

The following resolution was adopted by the Synod meeting of congregation representatives in February 2021:

> *The Synod acknowledges:*
> *The gospel calls us to relate to each other with love, treating each other with dignity and respect, and to condemn exploitation and abuse of vulnerable people. God's people are called to pursue justice including by empowering those who are exploited and abused.*
>
> *The covenanting relationship between the Uniting Church in Australia and the UAICC, as we pursue justice together.*
>
> *In our age, there is a need to prevent and address human rights abuses online, including acting against the promotion and facilitation of child sexual abuse.*
>
> *It is the role of Parliament, through the laws it passes, to provide the framework for how law enforcement agencies and the courts can access information and people's communication online. This is not a role for technology corporations.*
>
> *The Synod resolved:*
> *(a) To commend the Commonwealth Government for their preparedness to act to make the online world a safer place for everyone.*

(b) To call on the Commonwealth Government to ensure that the laws governing social media and the online world give law enforcement agencies the tools and budgets they need to prevent and address harms online. Such laws need to:

1. *Be effective and expedient to maximise the number of cases of harm that can be prevented and to ensure that evidence is not destroyed*
2. *Provide appropriate protections for the privacy of people not engaged in inflicting harm on others or criminal activity without undermining the ability of law enforcement agencies to address serious online harms;*
3. *Provide thorough oversight and transparency on how law enforcement agencies use the powers they are provided with; and*
4. *Provide adequate sanctions to deter any misuse of powers granted to law enforcement agents*

(c) To commend the Commonwealth Government for its resourcing of the e-Safety Commissioner to educate the community about online safety.
(d) To call on the Commonwealth Government to ensure Australian law enforcement agencies work effectively with overseas law enforcement agencies to investigate and gather evidence of child sexual exploitation that have partly or wholly taken place in Australia or involving Australian residents.
(e) To call on the Commonwealth Government to ensure Australian law enforcement agencies take reasonable steps to guarantee information provided to overseas law enforcement agencies will not itself be used to perpetrate human rights abuses.

Our view is that the harm caused by the ability of people to have completely anonymous identities online, where even the service provider does not know the real identity of the natural person using the service, far outweighs any benefits. There is almost no reason anyone in Australia needs to have an online identity where no one can identify them.

Some aspects of internet psychology have been studied since the 1990s and are well known and documented. The effect of anonymity online – or perceived anonymity – is one example. It has been found to fuel online disinhibition, that is, doing whatever you feel like as you are not worried about the disapproval of others. Disinhibition is fed by the perceived lack of authority online, the sense of anonymity, and the sense of distance or physical removal from others.[1]

Psychologist Jamil Zaki points out that anonymity tempts people to "try on cruelty like a mask, knowing it won't cost them. It does, of course, cost their targets."[2]

Due to the 'online disinhibition effect', as it is known, individuals can be bolder, less inhibited, and judgement impaired. Almost as if they were intoxicated. In this less-inhibited state, like-minded people can find one another quickly and easily, under a cloak of anonymity.[3] Cyber-psychologist Mary Atkin states about this behavioural amplification:[4]

> *But there are many incidences of risky behaviour becoming riskier online, especially pathological and criminal behaviour. Here's an example of what I mean: A stalker in the real world typically focuses on one victim at any given time, but a cyberstalker can stalk multiple victims simultaneously because technology makes that possible. Cyberstalking*

[1] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 21.
[2] Jamil Zaki, 'The War for Kindness. Building Empathy in a Fractured World', Robinson, 2019, 148-149.
[3] Mary Aiken, 'The Cyber Effect', John Murray Publishers, London, 2017, 5.
[4] Ibid., 23.

is considered an evolution of real-world criminal behaviour. Cyberspace is a breeding ground for mutations. Real-world behaviour migrates there and escalates or accelerates. This can sometimes have serious implications in the real world.

Child sexual abuse perpetrators operate in networks online to assist each other.[5] The anonymity that technology corporations allow online has permitted thousands of people to be part of such networks. The Virtual Global Taskforce online child sexual exploitation assessment of 2019 reported an increase in the number of organised forums and groups of offenders online in the preceding three years.[6]

In his speech to the National Press Club on 19 February 2020, the Commissioner of the Australian Federal Police, Reece Kershaw, stated that anonymity was a shield for those engaged in online facilitated child sexual abuse.

Being able to have anonymous identities online also assists child sexual abuse offenders in being able to assist each other, feeling that they can freely have conversations on online platforms and not be identified if the conversations were to be intercepted by law enforcement.

Analysis of conversations between child sexual abuse offenders in forums on the dark web that were captured in February 2021 found:[7]

- 32.8% of conversations were about the use of social media platforms;
- 13.5% of conversations were about content storage and exchange;
- 10.4% were about the use of direct messaging;
- 7.4% were about secure operating systems;
- 6% on how to capture live footage when a child has been coerced into conducting a sexual act;
- 1.5% on cloud file sharing; and
- 1.5% on image management.

The analysis shows the importance social media plays in the activities of those engaged in online child sexual abuse, compared to other issues.

The eSafety Commissioner publicly raised concerns in July 2021 that the chat app Kik allowed people to be completely anonymous.[8] The app allows people identified only by a username to share photos and videos. It also allows them to video chat and find or form chat groups. Ramiz Adam was able to log into Kik using anonymous identities and share child sexual abuse material with more than 4,000 users. Kik stated on their website they would only comply with US judicial requests and only provide transaction chat logs. The company deletes all video and images after 30 days, destroying evidence of the sharing of child sexual abuse on its platform.[9]

---

[5] Benoit Leclerc, Jacqueline Drew, Thomas Holt, Jesse Cale and Sara Singh, 'Child sexual abuse material on the darknet: A script analysis of how offenders operate', Australian Institute of Criminology, Trends & issues No. 627, May 2021, 7.
[6] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 15.
[7] WeProtect Global Alliance, 'Global Threat Assessment 2021', 28.
[8] Tessa Akerman, 'Paedophiles find prey in anonymous app', *The Australian,* 24 July 2021.
[9] Ibid.

The ease with which it is possible to set up multiple anonymous and false identities on social media platforms have greatly assisted those who seek to abuse children online. Those who seek to abuse children online can pose as a child themselves and groom a child to develop a friendship or romantic relationship with the child. Having established the relationship, the child is then manipulated into sharing sexually explicit images of themselves with the abuser.[10] The material shared is then used to blackmail more sexually explicit material, under threat of being shared with the child's friends or family.[11]

Examples of cases of alleged sexual extortion and grooming of children using false identities online

Muhammad Zain Ul Abideen

Perth man Muhammad Zain Ul Abideen Rasheed, 26, was sentenced to five years and four months in prison for sexually abusing a 14-year-old girl on 7 September 2021.[12] He has also been accused of engaging in the sexual extortion of 285 girls from Australia and around the world.[13]

He began sending sexually explicit messages to the girl he abused on Instagram in August 2019. Within eight days, he had met up with her twice and repeatedly sexually abused her after driving her to a local park.[14] After the first meeting with the girl, he gave her $115.

Mr Rasheed is facing over an additional 300 charges related to extorting sexual acts from girls across the world after he pretended to be a teenage social media celebrity to befriend girls online.[15] His lawyer was reported in the media as stating that Mr Rasheed plans to plead guilty to all the charges.[16]

He allegedly asked sexually explicit questions of the girls and the edited the written chat to change their answers. Police allege he would then threaten to send screen shots of the doctored conversations to their friends and family if they refused to provide nude photographs or perform live sexual acts on camera for him to watch. Police allege when the victim complied with the extortion, he would record the sexually explicit behaviour and threaten to release it to people they knew unless they then did more extreme acts.[17]

Timothy Patrick Cordova

[10] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan. Unclassified Version 2019', 2019, 14.
[11] Ibid., 14.
[12] Joanna Menagh, 'Muhammad Rasheed jailed for sexually abusing teenager amid hundreds of sextortion charges', ABC News, 7 September 2021, https://www.abc.net.au/news/2021-09-07/sextortion-accused-muhammad-rasheed-jailed-for-abusing-14yo-girl/100440312
[13] Paige Taylor and Paul Gravey, 'Alleged blackmailer faces more charges over young girls' online sex acts', *The Australian,* 23 April 2021.
[14] Joanna Menagh, 'Muhammad Rasheed jailed for sexually abusing teenager amid hundreds of sextortion charges', ABC News, 7 September 2021, https://www.abc.net.au/news/2021-09-07/sextortion-accused-muhammad-rasheed-jailed-for-abusing-14yo-girl/100440312
[15] Ibid.
[16] Ibid.
[17] Paige Taylor and Paul Gravey, 'Alleged blackmailer faces more charges over young girls' online sex acts', *The Australian,* 23 April 2021.

Timothy Patrick Cordova, a Victorian primary school teacher, pleaded guilty to 17 charges related to online child sexual abuse on 19 October 2021.[18] He admitted to using Instagram to receive child sexual abuse material between February and June 2020 11 times.[19] He pleaded guilty to soliciting images on the social media app three times and producing child sexual abuse material twice.[20] Fifty charges against him were dropped as part of a plea deal.

He posed as a teenage girl, Matilda Roberts, to allegedly entrap more than 70 boys.[21] He used the fake identity on Instagram to request sexual images from his victims.[22]

More than 60 of his alleged victims were past or present students from St Mark's Catholic Primary School in Dingley Village, with 26 of them being students he had taught.[23]

He was also accused to having taken naked photographs of children at a school swimming carnival.[24]

David Wilson in the UK
David Wilson had used fake social media accounts to trick at least 500 young boys into sending sexual videos and images of themselves, which he then used in extortion activities directed at them.[25]

Alladin Lanim
Alladin Lanim from Sarawak, Malaysia, had been sharing child sexual abuse material online since 2007. He was linked to more than 10,000 images and videos depicting the sexual abuse of children. He was able to hide behind an anonymous online profile. He was eventually identified in early 2021 and then located in July 2021. He was sentenced to 48 years in prison. Australian investigators identified 34 of the children he had abused, but there may be more.[26]

A common factor in a large proportion of cases of children being subjected to sexual extortion online is the ability of the perpetrator to use false identities on social media platforms to gain the trust of their victims.

---

[18] Frances Vinall, 'A Victorian primary school teacher has admitted posing as a teenage girl on social media for one disgusting reason', *NCA NewsWire,* 19 October 2021, https://www.news.com.au/national/victoria/courts-law/primary-school-teacher-timothy-patrick-cordova-admits-sick-trick-on-kids/news-story/f21bb57add5e67ab9e3cde7b979a6307
[19] Ibid.
[20] Ibid.
[21] Frances Vinall, 'A Victorian primary school teacher has admitted posing as a teenage girl on social media for one disgusting reason', *NCA NewsWire,* 19 October 2021, https://www.news.com.au/national/victoria/courts-law/primary-school-teacher-timothy-patrick-cordova-admits-sick-trick-on-kids/news-story/f21bb57add5e67ab9e3cde7b979a6307; and Rebekah Cavanagh and Ashley Argoon, 'Teacher arrest shock', *The Herald Sun,* 17 July 2020, 2.
[22] Rebekah Cavanagh and Ashley Argoon, 'Teacher arrest shock', *The Herald Sun,* 17 July 2020, 2.
[23] Ibid., 2.
[24] Ibid., 2.
[25] WeProtect Global Alliance, 'Global Threat Assessment 2021', 34.
[26] Chris Barrett, 'How Australian police tracked one of the world's most wanted paedophiles to Borneo', *The Age,* 5 September 2021.

Social media allows for the rapid dissemination of harmful slander and allows groups with hostile intentions to swiftly mobilise. It is difficult for innocent online participants to counteract this harm because the online space is primarily controlled by the social media companies who safeguard all their customers' privacy. Therefore it is challenging to remove false or misleading content targeted at human rights defenders.[27] The online experiences of human rights activists globally include many examples of online harassment with threats of violence (including sexual attack), baiting, doxxing, and public shaming. Women human rights defenders especially have been subjected to 'deepfake' videos in which their images and other images have been combined to present them in offensive ways. In addition, fake news, ' trolls', and hate speech have been used to campaign against human rights activists.[28] Completely anonymous identities have facilitated many of these abuses.

More than half of girls surveyed by Plan International for a 2020 report stated they had been harassed or abused online.[29] One in four girls abused online feels physically unsafe as a result.[30] Of girls who have been harassed online, 47% have been threatened with physical or sexual violence.[31] Their analysis of the situation was that:[32]

> *Perpetrators who threaten rape and physical violence, use abusive and sexist language, post manipulated photos and send pornographic pictures are able to remain anonymous and unconstrained; girls are often afraid, begin to restrict what they post and are forced to try and protect themselves.*

They correctly identify the anonymity that social media corporations provide to perpetrators of the abuse and harassment as a key factor facilitating the activity: “Perpetrators who would be subject to laws offline carry on with impunity and frequency with an empowering anonymity, online.”[33] Further:[34]

> *Girls and women often feel unsafe online but for the perpetrators it is different. Social media removes inhibitions. You can abuse people without consequences and without revealing your identity – for the harasser it is a very safe space indeed.*

Girls and women reported that in 36% of cases harassment was by a stranger, in 16% of cases it was by a group of strangers and in 32% of cases it was from an anonymous social media user.[35]

Online anonymity assists trolls in their efforts to hurt and harm vulnerable people. As one 'troll' told journalist Ginger Gorman, "Having morals, in general, is being soft. I find that humiliating people is fun but hurting them is hilarious."[36] He wanted people to feel unsafe online.[37]

---

[27] R.A.H. Zeid, ‘The impact of online violence on women human rights defenders and women’s organisations’, Statement by the UN High Commissioner for Human Rights, 38th session of the Human Rights Council, Office of the High Commissioner for Human Rights [OHCHR], Retrieved on 15.1.20 from https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23238&LangID=E, 2018 para 1 & 2.
[28] Front Line Defenders, ‘Front line defenders global analysis 2019’, Dublin, Ireland, 2020, 22.
[29] Sharon Goulds, Miriam Gauer, Aisling Cor and Jacqui Gallinetti, ‘Free to be online? Girl’s and young women’s experiences of online harassment’, Plan International, 2020, 7.
[30] Ibid., 7.
[31] Ibid., 17.
[32] Ibid., 7.
[33] Ibid., 9.
[34] Ibid., 23.
[35] Ibid., 26.
[36] Ginger Gorman, ‘Troll Hunting’, Hardie Grant Books, Melbourne, 2019, 12.

Gorman spoke to trolls that were part of packs that work together to try and get vulnerable people to harm themselves. They particularly target people with autism or mental illness. “Some people should kill themselves because they are generally pieces of shit,” one troll told Gorman.[38]

They also target rape survivors and the families of people who have recently died in tragic circumstances. For example, one troll told Gorman he was proud of upsetting the family of a young girl killed by a train by calling her a "train hugger".[39]

Romance scammers also make use of the anonymity social media platforms provide them with to fleece their victims, using false identities that cannot be traced to the real person behind the fake identity.[40] In 2019, Australians reported losing $29 million collectively through romance and dating scams.[41] It is the second highest form of criminal financial loss for individuals, after investment fraud.[42]

The overwhelming main benefit of the Bill will be that it will create an incentive of social media platforms to put in place systems to know who the natural person is behind each online identity. It creates that incentive by making the corporation liable for defamatory posts made on their platform. In addition, once the corporation knows who the real people are behind the online identities it will be possible for law enforcement agencies to identify people more quickly where that person is engaged in online human rights abuses that are criminal under Australian law. It will be far less likely that the social media platform will be unable to assist the law enforcement agency as a result of not knowing who the person behind an online identity is. It will also be harder for a person to use a fake identity to set up a social media account or accounts.

Defamation

Most of the public critique of the Bill by lawyers and legal academics is focused on what impact the Bill may have in relation to defamation cases. However, few of these people show any consideration for the positive impact the Bill would have in reducing the volume of anonymous and fake identities that are used on social media platforms for a range of serious human rights violations far more serious than many cases of defamation.

The Synod supports the aim of the *Social Media (Anti-Trolling) Bill 2021* Exposure Draft to make it clear that a person who owns a social media page is not the 'publisher' if defamatory comments are published on their page by third parties. We note the Bill is in response to the consequences of the High Court's decision in *Fairfax Media Publications v Voller* [2021] HCA 27 (*Voller).* However, we do note there will be some risk that the Bill may have the unintended effect of allowing extremist groups and people with extremist views to invite others to make defamatory comments on their social media pages in the belief that the Bill will provide them with a shield against any legal action that might be taken against them. The counter to this

[37] Ibid., 21.
[38] Ibid., 21.
[39] Ibid., 21.
[40] Karen Collier, ‘Romance rip-offs’, *The Herald Sun,* 14 February 2020.
[41] Ibid.
[42] Geoff Chambers, ‘Romance scammers in $60m swindle’, *The Australian,* 14 February 2020.

concern is that the social media service provider should deny service to people who invite others to make defamatory commentary.

Possible Amendments to the Bill

The Bill should be amended so that a provider must be forbidden from disclosing the identity or contact details of the complainant to the commenter.

The Synod would support that the provider of the social media service can also be compelled in other severe criminal and civil legal action, beyond defamation actions, to reveal the identity of the end-user accused of the illegal activity, with a penalty for the social media provider failing to do so.

Dr Mark Zirnsak
Senior Social Justice Advocate