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

29 College Crescent
Parkville Victoria
Australia, 3052

E-mail: digitalidentity@dta.gov.au

Uniting Church in Australia, Synod of Victoria and Tasmania submission on the Digital Identity Legislation Position Paper

16 July 2021

The Uniting Church in Australia, Synod of Victoria and Tasmania, welcomes this opportunity to provide feedback on the *Digital Identity Legislation Position Paper.*

The Synod's membership is concerned about serious harms being facilitated in the online world. Therefore, at the February 2021 Synod meeting of representatives of congregations across Victoria and Tasmania, the members unanimously adopted the following resolution:

> *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.*
>
> *That the Synod resolves:*
>
> *(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:*
>
> - *Be effective and expedient to maximise the number of cases of harm that can be prevented and to ensure that evidence is not destroyed;*
> - *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;*

- *Provide thorough oversight and transparency on how law enforcement agencies use the powers they are provided with; and*
- *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.

(f) To inform the Prime Minister, the Minister for Home Affairs, the Minister for Communication, Cyber Safety and the Arts, the Leader of the Opposition, the Shadow Minister for Home Affairs, the Shadow Minister for Communications and the Leader of the Greens of this resolution.

The Uniting Church in Australia has stated its support for international human rights instruments, including the right to privacy. The Synod recognises that the right to privacy must be upheld in consideration of other fundamental human rights. The right to privacy cannot be used as a shield to conceal other human rights abuses a person or entity is involved in.

Therefore, the key issue we would wish to raise on the digital identity legislation is that it is designed to avoid people wanting to carry out human rights abuses and crime online being able to use the system to create identities where there is not a natural and identifiable person behind the digital identity. The system must be robust enough that the natural person behind the digital identity has been verified by someone, and law enforcement agencies would be able to identify the person if they had a legitimate reason to do so. Further, the system should not inhibit entities required by law to do due diligence on the people they deal with from being able to conduct that due diligence by creating an impenetrable shield that blocks necessary due diligence. For example, such a due diligence obligation exists for reporting entities under the *Anti-Money Laundering Counter-Terrorism Financing Act 2006.*

In the online world, millions of people globally engaged in serious criminal activities that harm other people at every moment in time. The more we allow people to have anonymous identities online, where nobody knows who the natural person behind the online identity is, the harder and harder it becomes for police to catch such people. The combination of entirely anonymous identities, communication channels that police cannot access in any circumstances and technology corporations being able to conceal and destroy evidence of serious crimes creates an online environment where those wishing to harm others can have a sense of impunity. This encourages higher levels of severe criminal behaviour. The higher levels of serious criminal behaviour mean that police can deal with a shrinking portion of the online criminal behaviour, which in turn increases the level of people engaged in serious criminal conduct. It becomes a vicious circle.

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 through fake identities – 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]

Thus under 7.4.3 Restrictions on data profiling, an exemption should apply where Accredited Participants should be permitted to collect, use and disclose information about a User's behaviour on the system to meet a legislative requirement relating to the prevention of criminal activity (such as anti-money laundering requirements).

Under section 7.4.6 Requirement to express consent, should not apply where seeking the User's consent would tip them off they are being investigated for suspected severe criminal activity. Tipping someone engaged in illegal activity off could result in them being able to destroy or conceal vital evidence and evade arrest by law enforcement agencies.

We support the proposal in 7.4.8 that Accredited Participants retain metadata and activity logs for a period of seven years for the purpose of maintaining the integrity of the system, which should include fraud and criminal investigation purposes.

The Synod supports the proposal in 7.4.11 that the minimum age for the use of a Digital Identity in the system is 15 years of age. We also support that the Oversight Authority will be able to override the default minimum age limit in circumstances where it considers it appropriate.

Dr Mark Zirnsak
Senior Social Justice Advocate
Phone: 0409166915
E-mail: mark.zirnsak@victas.uca.org.au

[1] Ibid., 21.
[2] Jamil Zaki, 'The War for Kindness. Building Empathy in a Fractured World', Robinson, 2019, 148-149.