



Catholic Women's League Australia Inc
Member Organisation of the World Union of Catholic Women's Organisations (WUCWO)
NGO Consultant (roster) status with the Economics and Social Council of the United Nations

"To make Jesus, our loving Saviour, and Mary, our Blessed Mother, better known and loved"

Trusted Digital Identity System Bill **Submission**

Introduction:

On behalf of the members of the Catholic Women's League Australia Inc., we urge care and extreme caution with the implementation of a Bill that contains vague conditions and cannot even stipulate the method and means through which such a System would be implemented, governed and secured.

We acknowledge that in this digital age further development and action needs to be taken to build the "missing layer of trust"ⁱ through which ID Providers supply a Digital Identity to Relying Parties. We understand that, in order for Australia to continue as a thriving democracy, we need to develop better governance of our cyber activity to ensure security, interoperability, and legal requirements that can operate effectively within our jurisdiction and have the capacity to interact with jurisdictions world-wide.

However, after consultation with a number of knowledgeable people in the Digital Identity field, we have grave concerns about the Third Phase of the Bill and believe that it is built upon a faulty platformⁱⁱ that will not deliver the necessary safety & security of Digital Identity data, nor ensure the civil liberties of Australians. Our questions and concerns, which are germane to lawful storage and the handling of personal data under a digital identity, are presented under the themes below.

1. Data ownership and storage:

- Who retains ownership of our personal digital identity?
- Where will the data be stored?
- Can the Government ensure that the data will continue to be stored in Australia and not be left to "good-faith" if outsourced to third party providers?
- If data is stored in Australia and subject to Australian data privacy laws, what safeguards are already in place to prevent cyber attacks on servers – which have already proven to be vulnerable to attack and data theft?
- Who is liable if the data is "lost", stolen and misused?
- The collection of attributes and biometrics is often outsourced to other stakeholders – where do those *onboarded* entities store their information; and how will the veracity of claims of compliance by cross border entities with Australian privacy laws be confirmed? This is especially troubling if the private entities are afforded the self-governance suggested in the legislation.
- What are the protected "attributes" and who puts a limit on them – for example, the mining of emotional attributes?

2. National Security:

All Correspondence to Catholic Women's League Australia (Inc)
PO Box 176, Sandringham, Victoria, 3191

email: cwla.info@gmail.com



ABN 91323005375

Catholic Women's League Australia Inc

Member Organisation of the World Union of Catholic Women's Organisations (WUCWO)
NGO Consultant (roster) status with the Economics and Social Council of the United Nations

"To make Jesus, our loving Saviour, and Mary, our Blessed Mother, better known and loved"

- Australia continues to remain vulnerable to cyber attack, and our system is not yet robust enough to handle a whole-of-economy move toward Digital Identity centralisation and roll out.ⁱⁱⁱ
- The recent outage of Facebook/Instagram/WhatsApp for 6 hours caused by a coding error demonstrates the vulnerability of an internet platform that turns over 89 billion per annum and has many thousands of engineers available to correct errors – how fit is Australia to deal with such a human error, let alone a major cyber attack?

3. The "Right to be forgotten":

- Europe and other nations have enacted a "right to be forgotten" law, enabling individuals to retain the sovereign ownership of their digital information with the right to instruct immediate wiping of information once permitted use is complete.
- Australian law lacks this civil liberty and the right to remain private and unseen by government and other *onboarded* entities.
- Worryingly this Bill "allows for the retention of biometric information...to enable operational testing and fraud detection". This vague and even alarming allowance has no place in a free democracy.
- We live in an economy still reliant upon "good faith but driven by profiteering and the marketing of services through the use of "scraped" or mined information from the individual. Can the government clarify whether they intend to prohibit the scraping of personal information by the System and "forget" the users once they have finished utilising a private or government service?

4. The Problem of Opt-in as the default position:

- Frequently, Australians are obliged to opt-out of a system that they may never have realised they were opted into. For example – our vaccination status, our personal health records, R-rated settings on phones, the availability of porn on our computers, biometric data bases – such as the data base of driver's licences in Victoria, and now, this Digital Identity System and its proposed frameworks.
- Therefore, the Trusted Digital Identity System needs to be set up to be *at the service* of the citizens – should they wish to opt-in and use it, or not.

5. Coercion, access and equity:

- Our concern is that, in spite of the Bill suggesting that it must remain voluntary; increasingly Australians are being shut out of society if they do not choose to follow the mandates and processes of increasingly strident governments.
- This Bill must enshrine the absolute right of the individual to choose the method for identification– with all of the safeguards in place to ensure that this government, its oversight authorities, and government services have no means to coerce or misuse any information to which they have access.
- We believe that it becomes dangerous when a government is given power over the centralised verified digital documents of its peoples.
- Therefore, the proposed Bill needs to clarify how the Oversight Authority will utilise decentralised and encryption technologies, such as blockchain and zero knowledge proofs, to decentralise and secure the private information of the users and enable a detailed log of all agencies – government and otherwise – who have accessed the information.

**All Correspondence to Catholic Women's League Australia (Inc)
PO Box 176, Sandringham, Victoria, 3191**

email: cwla.info@gmail.com



ABN 91323005375

Catholic Women's League Australia Inc

Member Organisation of the World Union of Catholic Women's Organisations (WUCWO)
NGO Consultant (roster) status with the Economics and Social Council of the United Nations

*"To make Jesus, our loving Saviour, and Mary, our
Blessed Mother, better known and loved"*

In conclusion, the Catholic Women's League Australia Inc. believes that the proposed legislation is purposefully sloppy, vague and unclear about how it proposes to govern, protect and respect the privacy and civil liberties of Australians, how it means to protect and secure the digital data and respond to inevitable cyber attacks, and finally, how it means to prevent any future governing bodies from an Orwellian nightmare and an attack upon the rights and freedoms of individuals of this great country.

Yours Sincerely,

Katrina Mathai
National President, Catholic Women's League Australia Inc.
October, 2021.

ⁱ <https://www.csoonline.com/article/3405120/is-the-digital-identity-layer-missing-or-just-misplaced.html>

ⁱⁱ <https://www.zdnet.com/article/researchers-want-australias-digital-id-system-thrown-out-and-redesigned-from-scratch/>

ⁱⁱⁱ <https://www.abc.net.au/news/2021-01-11/australians-turning-point-on-cyber-security-cyberattacks-crime/13018884>