This is my submission to the Digital ID Bill 2023.

Because I do not own a smartphone, and have no intention of ever owning a smartphone, a digital ID system does nothing to make my life streamlined and convenient. However, I would be greatly inconvenienced if workarounds for circumventing a Digital ID system were either unworkable or inconvenient.

If a Digital ID system is introduced, then I strongly believe that it should be a voluntary 'opt-in' arrangement, rather than being mandatory or 'opt-out.' In particular, I do not believe that Digital ID should be made mandatory for vulnerable groups such as welfare recipients and survivors of natural disasters. Overseas, there have been cases involving out-of-touch assumptions that everyone eligible for natural disaster aid is a smartphone owner, and this fails to take account of poverty and growing cost-of-living pressures.

Digital ID will be intimately linked to biometrics, with users obliged to upload a biometric scan of their face. This use of sensitive and personal biometric information is likely to be mandatory for any Digital ID to be established.

The collection of such sensitive information brings up a list of concerns, which include:

- The privacy rules governing such scans, and whether these scans would be used without the individual's explicit permission for other biometric identification purposes, or for biometric surveillance imaging.
- Whether or not biometric data is stored, and whether this would only occur if strictly necessary.
- The privacy policies of any third-party company creating backups or offering cloud services for biometric data.
- Changes in the privacy policies of these companies, the smallest of which would need to be overseen, and if necessary, negotiated with the relevant government department.
- Whether state of the art protection against hackers would be employed by the Australian Government and by third-party companies, and in the case of these companies, how this can legally be independently monitored and overseen.

If a Digital ID system exists, then it would be necessary to strictly limit the reasons for ID information being used or accessed by any participating government agency or business, there would need to be a mechanism that prevents law enforcement from accessing the data, and such a system should not be used for age verification.

If a scenario were to arise where a Digital ID system is required to access social media and online banking, for example, then I would automatically discontinue my use of social media, and look for ways to avoid online banking, despite the inconvenience involved.

In the broader world picture, voters are increasingly keen on voting for far-right parties with authoritarian streaks, and in some countries these are already in government. For an

authoritarian regime that has starting along the path of abusing its citizens' human rights, the possession of sensitive biometric information via Digital ID systems represents a serious risk.

In its 2022 report *Advancing Digital Agency: The Power of Data Intermediaries*, the World Economic Forum, a key Digital ID advocate, reveals on p23 that it sees transhumanism (in the form of body-embedded implants) as one long-term goal of its overarching Digital ID agenda. Whether or not the Australia Government shares these same visions, it is understandable that many people who look below the surface of this topic will be wary of its potential Frankenstein/cyborg applications. Indeed, unguardedly transhumanist language was used by Mastercard in its promotional material for a face biometric payment system, which refers to the merging of the physical and digital worlds.

This Digital ID initiative is a key plank in the shift towards a technology-dominated dystopian technocratic world in which more power and control is concentrated in the hands of governments and technology giants. Such an outcome cannot be good for society as a whole.