Submission on the Digital ID Bill 2023

Dear Committee Secretary,

Consultation on the Digital ID Infrastructure

1. I write as part of the consultation for the proposed bill titled '*Digital ID Bill 2023'* (**bill**).

Summary

2. The key issues with the bill are as follows:

   a) **Foreign Interference:** Opens the doors to foreign interference and cyberattacks
   b) **Liability Issues**: Liability provisions for companies in breach is vague
   c) **Offshore Data Concerns**: Allows for offshore data storage and transfer
   d) **Privacy Concerns:** Impinges upon privacy rights of citizens
   e) **Coercive model:** May be coercive and not 'voluntary' as promoted in the bill

Author details and background

3. I am writing this submission on behalf of Christian Faith and Freedom Inc., as a citizen with a *juris doctor* degree. I have an interest in human rights and privacy legislation and have given a presentation on privacy and technology, at Curtin University's symposium on *Law, Technology and Labour Governance* conducted in 2020. I have written numerous publications concerning legislation, law and policy.

4. I have no relevant conflicts of interest. I write in my personal capacity as a private researcher affiliated with CFF which provides advocacy and aid for people subjected to discrimination and persecution for their faith and ethnicity overseas, and engages in human rights issues of public concern in Australia.

a) Foreign Interference

5. Warfare of the 21st century is largely conducted in cyberspace. There are tremendous issues which arise in nations wishing to rely upon or engage in more digital models, including the rise in cybercrime, misuse of data, fraud and identity theft. China is one of the world's leading suppliers of digital infrastructure and technology – servers or other infrastructure stored offshore can be attacked or co-opted by foreign actors, meaning a reliance on cybertechnology can become extremely problematic in the event of a cyberattack. Identity fraud is amongst Australia's top three cybercrimes.

6. Foreign actors may also hack data and use it for malevolent purposes contrary to Australia's national interests. The amount of data collected and stored online, with the digital ID infrastructure, will mean Australia's sensitive information will be in a location where foreign actors with advanced hacking capabilities can access it more easily. Australia's current cybersecurity is not as advanced as it should be, to deal with threats such as the Chinese Communist Party which has more advanced cyber capabilities.

b) Liability Issues

7. The government will not be adequately penalized under a liability issue resulting from a contravention of the Act as section 158(5) indicates the maximum penalty that a court can order for a government body in breach, is 5 times the pecuniary penalty specified for the civil penalty provision. If this is tax cash paid for a breach, there is no real penalty the government suffers for a contravention of the Act, and there is no real incentive to stop government malpractice and contravention, if there is only a soft monetary penalty applied.

8. Secondly, section 159 titled 'protection from civil action,' appears to soften the liability a person acting in contravention to the Act will suffer. A person is 'not liable to an action or other proceeding for damages for, or in relation to, an act done or omitted to be done in good faith by the person in their performance under the Act, or in the exercise of any powers under the Act.' Limiting liability of the ID regulator and other related persons managing the digital ID infrastructure fosters immediate public distrust over the bill and overall framework.

9. Thirdly, Section 160 is poorly drafted and demonstrates little concern over Australia's national security as it limits civil penalties for those who contravene a civil penalty provision if the conduct occurs wholly in a foreign country. This is questionable drafting as it appears to protect foreign entities, particularly at subsection 3 which states 'despite subsection (1), an entity does not contravene a civil penalty provision of this Act if: a) the alleged contravention is an ancillary contravention; and b) the conduct constituting the alleged contravention occurs wholly in a foreign country, but not on board an Australian aircraft or an Australian ship…d) the entity is not an Australian entity; and e) there is not in force, in the foreign country or the part of the foreign country where the conduct constituting the alleged contravention occurred, a law creating a pecuniary or criminal penalty for conduct corresponding to the conduct constituting the primary contravention to which the alleged contravention relates.'

10. Section 84 is negligently drafted and offers no real citizen protection over a breach or contravention of the Act caused by an accredited entity. Section 84 states 'accredited entities participating in the Australian Government Digital ID System protected from liability in certain circumstances,' indicates lax liability for breaches. Further subsection 1 of section 84 indicates if matters are conducted in 'good faith' there is no liability for a contravention by an accredited entity. Practically speaking, an entity can easily pretend to be operating in 'good faith' and contravene the bill, and thus be protected from liability. The liability provision therefore should include detail about who will determine whether conduct was done 'in good faith' or not. The digital ID regulator is assumed to be the investigator of a contravention. The digital ID regulator therefore, should be an independent body to any accredited entity and have no ties whatsoever, or conflicts of interest, to accredited entities participating in the digital ID system. This will allow for liability investigations to be conducted fairly and respectfully, with priority being given to citizens rather than companies in breach.

c) Offshore Data Concerns

11. Nowhere in the bill does it explicitly indicate that data cannot and should not be held outside of the jurisdiction of Australia. The digital ID infrastructure is supposedly guarded from cyberthreats however The Chinese Communist Party and other foreign entities may have better cyber capabilities than Australia is currently aware. Holding data offshore is a national security threat, or having private entities based outside of the jurisdiction holding Australian citizen data is precarious. The scope of data that can be collected is broad in the

bill; it includes biometric data. This kind of data can be hacked and used for malevolent purposes. Tracking the transactions of citizens or government entities within Australia is something foreign actors will have interests in. Data should therefore be secured within the Australian jurisdiction under domestic security infrastructure or the security of trusted allies. If foreign jurisdictions such as China are linked to some degree to any of Australia's digital ID infrastructure, this needs to be re-evaluated. Many private companies within Australia have ties to China, and Chinese law governs commercial businesses operations in and outside of China, if the company is registered as Chinese.

12. The digital ID infrastructure, if it is to be enacted, must be done completely independently of foreign actors. If this is not the case, we may get a 'Huawei' situation. Australia banned *Huawei* from its 5G network in 2018.

d) Privacy Concerns

13. Many citizens are not comfortable with the scope of data that can be collected under the bill. The argument is to 'streamline' online transactions and business, however any kind of data being held in a digital space has the capacity to be misused, despite the government attempting to secure it. Biometric data collection for purposes other than medical, may be an invasion of privacy and contrary to the ICCPR, particularly at article 17 which states:

    'No one shall be subjected to arbitrary or unlawful interference with his privacy…everyone has the right to the protection of the law against such interferences or attacks.'

14. The bill also contradicts its supposed concern for citizen privacy by limiting liability to breaching entities. For example at section 44 (1), the collection of certain attributes of individuals is prohibited except subsection 1 does not apply if the accredited entity themselves did not solicit the attribute of the individual or destroys the attribute as soon as practicable. This is poor and vague drafting that does not adequately protect citizens as it allows a related entity to the accredited entity to take data from citizens, if there is a capacity for a related entity to gain access to data. There should be penalties attached to a breach of this nature to incentivise companies to better protect data and avoid the collection of data that is prohibited.

e) Coercive Model

15. In division 5 of the bill titled 'Other Matters relating to the Australian Government Digital ID System,' there is an 'exemption' section at s 74(4) which states 'Subject to subsection (6), the Digital ID Regulator may, on application by a participating relying party, grant an exemption under this subsection to the participating relying party if the Digital ID Regulator is satisfied that it is appropriate to do so.' This indicates there is nothing purely voluntary about the digital ID system. It may be coercive or even mandatory, if the exemption provision aforementioned, is relied upon. This section needs to be amended or removed so that the digital ID system is truly voluntary as it is being promoted as such, by the government currently, otherwise these claims are misleading to the public.

16. Section 71 of the bill indicates that the ID system is 'voluntary' (subsection 1) however this does not apply to a service of a participating party if the service provides access to another service, for example. This demonstrates a mere illusion of 'voluntariness' for

citizens. No coercion at all should be used and no framework allowing for coercive methods should be used.

Objections to the Aforementioned Arguments

17. The bill argues it is concerned for citizen privacy rights however the lax drafting as argued above in regard to limiting the liability of entities in contravention to the Act demonstrates citizen protections are not safeguarded adequately, or as convincingly as is being promoted.

18. The bill offers some protection for citizens who have found their data has been misused by breaching entities. However, realistically, how will a citizen be notified of a data breach? The bill should contain provisions which adequately safeguard citizens when breaches occur insofar that if government or a regulatory body finds a data breach or another type of breach, affected citizens should be alerted and should have the option to be compensated adequately and to opt out of the digital ID system without hassle.

19. The bill appears to value security, however, there is no guarantee that entities with better cyber capabilities than Australia will not engage with Australia's digital ID system for their own purposes which is outside of the government's control.