QUEENSLAND COUNCIL FOR CIVIL LIBERTIES

Protecting Queenslanders' individual rights and liberties since 1967

Watching Them While They're Watching You

9 October 2023

[redacted]

By eLodgment

[redacted]

RE: 2023 DIGITAL ID ACCREDITATION

---

1. The Queensland Council for Civil Liberties ("**the QCCL**") is a not-for-profit organisation that promotes civil liberties and receives queries from members of the public regarding their civil liberties and individual rights.

2. We make this submission in response to *Digital ID Bill 2023* and Digital ID Accreditation Rules ("**the ID Accreditation Bill**").

3. We have **attached** a copy of our submissions made in response to the Digital Transformation Agency ("**the DTA**") public consultation regarding the *Trusted Digital Identity Bill 2021* ("**our TDIF Submission**").

4. We appreciate that the ID Accreditation Bill is not identical to the *Trusted Digital Identity Bill 2021*; however, we submit that our position generally stated in our TDIF Submission has equal application to the instant consultation. In essence, that submission was that:

    a. the implementation of a digital identity scheme in Australia is a significant step and it is imperative that this is approached in a way that is measured, transparent, comprehensively safeguarded and that the Australian community is fully informed as to all potential consequences of this path; and

    b. there are benefits that may be derived from a digital identity system in Australia; however, those benefits must be couched with clear and enforceable safeguards.

5. We consider that this is a balanced and reasonable position that measures the benefits for Australians against potential harm(s) that may arise from implementing a

system into Australia law which will irretrievably alter the way that many Australians interact with government (and providers accredited under the Rules).

6. In our TDIF Submission, it was our position that:

> *... it is our submission that the Bill should not be progressed until at least the following has occurred:*
>
> *a. an enforceable Federal human rights framework has passed into Australian law;*
>
> *b. a public electoral campaign is held that brings the introduction of the Bill to an election;*
>
> *c. further consultation is undertaken as to the operation of the Bill and the impact on Australians; and*
>
> *d. public awareness polling occurs to ensure that the Bill and its operation is desirable to the Australian community.*
>
> *It is our position that, although benefits could be inferred from the Bill, this legislation creates such a significant change to Australian life and the way in which Australians choose to identify and exchange identity that it warrants being taken to an election. In our view, the Federal Government is positioned to run this campaign and that process would significantly assist the Government in being able to make a genuine promise to the Australian community that the TDIF and Digital Identity arrangements can be trusted and that they are desirable to the Australian community.*
>
> *In our view, put bluntly, if this arrangement is not taken to the Australian community via an election campaign, it will erode the trust required for this system to properly operate and demonstrate that the Bill is being introduced based on assumption rather than informed knowledge that the Bill is desirable.*

7. We observe that our submission that the implementation of a digital identity scheme was *not* taken to the Australian public at the 2022 Federal election.

8. We also note that there are curious changes in the ID Accreditation Bill that are stark differences in drafting of core concepts in the *Trusted Digital Identity Bill 2021*. For example, we note the following changes to the definition of *attribute of an individual*.

9. In the *Trusted Digital Identity Bill 2021*, section 10(3) provided that the following is <u>not</u> an attribute of an individual:

> *(a) biometric information of the individual;*
> *(b) a restricted attribute of the individual;*
> *(c) information or an opinion about the individual's:*
> *a. racial or ethnic origin; or*
> *b. political opinions; or*
> *c. membership of a political association; or*
> *d. religious beliefs or affiliations; or*
> *e. philosophical beliefs; or*
> *f. membership of a professional or trade association; or*
> *g. membership of a trade union; or*
> *h. sexual orientation or practices; or*
> *i. criminal record;*
> *(d) information that is prescribed by the TDI rules and relates to 12 the individual.*

10. Section 10(4) of the *Trusted Digital Identity Bill 2021* provided that "*subsection (3) does not prevent information described in any of the paragraphs in subsection (2) from being an attribute of an individual if the information is not primarily of any of the kinds described in subsection (3), even if information of any of those kinds can reasonably be inferred from the information*".

11. However, these matters appear now to be specifically included as attributes of an individual. Indeed, the ID Accreditation Bill goes further and now provides the following at section 10:

> *(1) An attribute of an individual means information that is associated 8 with the individual, and includes information that is derived from 9 another attribute.*
>
> *(2) Without limiting subsection (1), an attribute of an individual 11 includes the following:*
>
> *(a) the individual's current or former name;*
> *(b) the individual's current or former address;*
> *(c) the individual's date of birth;*
> *(d) information about whether the individual is alive or dead;*
> *(e) the individual's phone number;*
> *(f) the individual's email address;*
> *(g) if the individual has a digital ID—the time and date the 19 digital ID was created;*
> *(h) biometric information of the individual;*
> *(i) a restricted attribute of the individual;*
> ***(j) information or an opinion about the individual's:***
> ***i. racial or ethnic origin; or***
> ***ii. political opinions; or***
> ***iii. membership of a political association; or***
> ***iv. religious beliefs or affiliations; or***
> ***v. philosophical beliefs; or***
> ***vi. sexual orientation or practices.***
>
> (our emphasis)

12. As the DTA would appreciate, this is a significant expansion (indeed, it encompasses previously excluded information) of the definition of "attribute". Given that this definition is critical to the *ID Accreditation Bill*, and although we trust that this re-drafting has occurred for the purpose of a wider coverage of the privacy principles to accredited entities (as provided at s 33 of the *ID Accreditation Bill*), we question why this has been expanded and seek that the Government provides more clear information regarding this definition in the context of our primary submission recited at paragraph six (6) herein.

13. Further in the context of the immediately preceding paragraph, we note that the Government has recently released its response to the Privacy Act Review Report wherein the Government has responded that it will immediately implement many of the recommendations contained in that report and committed, in principle, to the vast majority of the recommendations.

14. Given that the implementation of the Privacy Act Review Report recommendations has a fundamental bearing on the *ID Accreditation Bill* and further noting the current

review of Australia's Human Rights Framework[1], we consider that it would be most appropriate to delay the introduction of the *ID Accreditation Bill*.

15. We trust that these submissions assist the consultation and the ID Accreditation Bill generally and we confirm that we are willing to assist further with any public hearing(s) associated with this process.

16. Please do not hesitate to contact us should you require any further information.

[1] Australian Government, 'Australia's Human Rights Framework', https://www.aph.gov.au/-/media/Committees/Senate/committee/humanrights_ctte/Aus_Human_Rights_Framework/Aust_HR_Framework_2010.pdf?la=en&hash=E28A006D823EE0BCDDCED2C0B851C4E56B4EEE04, accessed 2 June 2023.

QUEENSLAND COUNCIL FOR CIVIL LIBERTIES

Protecting Queenslanders' individual rights and liberties since 1967

Watching Them While They're Watching You

14 October 2021

[redacted]

[redacted]

Dear Minister,

RE: Exposure Draft on Australia's Digital Identity Legislation

1. The Queensland Council for Civil Liberties ("**the QCCL**") is a not-for-profit organisation that receives queries from members of the public regarding their civil liberties and individual rights.

2. The Digital Transformation Agency ("**the DTA**") may appreciate that the writer has been involved with the development of the Bill from its inception and attended numerous roundtables regarding the development of the Bill. We appreciate the opportunity to provide further feedback on the *Trusted Digital Identity Bill 2021* ("**the Bill**").

3. At the outset, it must be understood that the Trust Digital Identity Framework ("**TDIF**") and the implementation of the Bill is a *significant* step being contemplated and it is imperative that this is approached in a way that is measured, transparent, comprehensively safeguarded and that the Australian community is fully informed as to all potential consequences of this path being considered.

4. In this vein, we appreciate that there are benefits that may be derived from the Bill and implementation of the TDIF in Australia. Those benefits could be realised for disabled persons, disenfranchised persons and welfare recipients. However, those people also require the strongest safeguards and protections.

5. In this submission, we provide our view on:

    a. the landscape within which the Bill has been introduced; and

    b. issues with the Bill.

[redacted]

6. In this submission, we have not made recommendations regarding specific amendments that could be made to the Bill because it is our submission that the Bill should not be progressed until at least the following has occurred:

    a. an enforceable Federal human rights framework has passed into Australian law;

    b. a public electoral campaign is held that brings the introduction of the Bill to an election;

    c. further consultation is undertaken as to the operation of the Bill and the impact on Australians; and

    d. public awareness polling occurs to ensure that the Bill and its operation is desirable to the Australian community.

7. It is our position that, although benefits could be inferred from the Bill, this legislation creates such a significant change to Australian life and the way in which Australians choose to identify and exchange identity that it warrants being taken to an election. In our view, the Federal Government is positioned to run this campaign and that process would significantly assist the Government in being able to make a genuine promise to the Australian community that the TDIF and Digital Identity arrangements can be trusted *and* that they are desirable to the Australian community.

8. In our view, put bluntly, if this arrangement is not taken to the Australian community via an election campaign, it will erode the trust required for this system to properly operate and demonstrate that the Bill is being introduced based on assumption rather than informed knowledge that the Bill is desirable.

<u>The landscape within which the Bill has been introduced</u>

9. The QCCL has made submissions to a large number of legislative reforms attempting to grapple with the rapidly expanding digital landscape in Australia.

10. Currently, the Bill may be impacted or may be consequentially affected by the following recent legislative developments:

    a. the passage of the *My Health Records Amendment (Strengthening Privacy) Act 2018*;

    b. the passage of the *Assistance and Access Act 2018*;

    c. the passage of the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021*;

    d. the passage of the *Telecommunications Legislation Amendment (International Production Orders) Act 2021*;

    e. the *Corporations (Director Identification Numbers—Transitional Application Period) Instrument 2021* made 29 September 2021;

    f. *Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019* and the Parliamentary Joint Committee on Intelligence and Security's Advisory Report issued in October 2019 recommending that that Bill be re-drafted;

    g. the review of the *Privacy Act 1988* announced by the Attorney-General's Department on 12 December 2019; and

    h. the introduction of the *Data Availability and Transparency Bill 2020* on 9 December

2020.

11. As the QCCL has repeatedly submitted to Parliamentary inquiries, including the abovementioned legislative developments, Australia lacks an enforceable Federal human rights framework. Absent of such a fundamental safeguard, any legislation that has the potential to impact Australians' human rights ought to be held in abeyance until such a framework has been developed and entered force.

Issues with the Bill

12. Firstly, we submit that the TDIF Rules should be entrenched within the legislation itself and it is inappropriate to have, as s. 157 of the Bill provides, such a fundamental aspect of the Bill existing merely within a legislative instrument(s). While we accept that s. 158 of the Bill tempers our concern by the requirement for consultation prior to the making or amending the TDIF Rules, those TDIF Rules have such a fundamental consequence upon the trust of the arrangements proposed in the Bill that they ought to require parliamentary passage before alteration unless in an emergency. This first concern is amplified by the effect of s. 158(7) of the Bill that provides that a failure to consult does not invalidate the TDIF Rules (or any other legislative instrument).

13. We are concerned to ensure that if the Bill is progressed, it only occurs on the basis of a genuine (rather than implicitly required) bargain of trust being brokered between the citizen and the State.

14. In this context, we consider that the following points require further consideration before these aspects of the Bill become law:

    a. Although we appreciate that the objects contained at s. 3 of the Bill require contemplation of the potential benefit of a digital identity for Australians, it is our submission that the protection of Australians ought to be the paramount object of this legislation with any economic benefit being expressly subordinate to the protection of Australians' personal information.

    b. It is not entirely clear how the extraterritorial operation expressed at s. 7 of the Bill would interact with other legislation, such as mutual legal assistance treaties or the *Telecommunications Legislation Amendment (International Production Orders) Act 2021* and it ought to be made express that Australians' personal information (including any metadata retained in the course of the operation of the TDIF) is not made available to domestic or foreign law enforcement agencies.

    c. We submit that the penalty of 200 penalty units for offences contained at s. 15(2) and (3) of the Bill relating to unauthorised or unlawful connection to the trusted digital identity system is insufficient and this penalty ought to be significantly increased to reflect the significant harm that may be caused by unauthorised or unlawful access to Australians' personal information.

    d. The conditions for approval to be onboarded to the trusted digital identity system (ss. 18, 21, 22 and 24 of the Bill) ought to include express consideration as to the entities' ability to ensure security for Australians' personal information and consideration as to the entities' past compliance with the *Privacy Act 1988* and the common law obligation of confidence. Further, we submit that it is inappropriate to leave those consideration to the TDIF Rules. This submission has equal application to s. 59 of the Bill.

    e. Participation in the trusted digital identity system must be voluntary and the exception to s. 30(1) of the Bill contained at s. 30(2) ought to be removed.

f. Section 31 of the Bill regarding holding of digital identity outside of Australia ought to be amended to expressly prohibit holding, storing, handling or transfer of digital identity information outside Australia. We further submit that the penalty of 300 penalty units for offences contained at s. 31(3) of the Bill relating holding, storing, handling or transfer of digital identity information outside Australia is insufficient and this penalty ought to be significantly increased to reflect the significant harm that may be caused by unauthorised or unlawful (foreign) access to Australians' personal information.

g. The Trusted Provider Agreements contained at s. 35 ought to be the subject of statutory obligation for transparency and users ought not be financially burdened by the operation of the TDIF. This submission has equal application to ss. 140 and 144 of the Bill.

h. The exclusion of liability contained at s. 39 of the Bill is inappropriate and liability should not be excluded as accountability is fundamental to the development of trust required in the TDIF.

i. The penalty for failing to contact affected individuals as a consequence of a digital identity fraud incident or cyber security incident provided at s. 43(2), (3) and (6) is manifestly insufficient and the penalty of 200 units for ought to be *significantly* increased to reflect the significant harm that may be caused to a person as a consequence of either or both a digital identity fraud incident or cyber security incident.

j. The obligation to deactivate a digital identity contained at s. 61 of the Bill ought also include an obligation to deactivate any secondary or ancillary existence of an individual's digital identity retained, directly or indirectly, in the TDIF.

k. The Federal Government must make an irrevocable agreement to increase the budget for the Information Commissioner so as to ensure that the oversight function for the Information Commissioner at ss. 70, 71 and 72 of the Bill can be properly performed.

l. The penalty for failure to obtain express consent contained at s. 73 and 74 of the Bill of 200 units for ought to be *significantly* increased as accountability is fundamental to the development of trust required in the TDIF.

m. The penalty for failure to delete biometric information after processing contained at s. 79(5) of the Bill of 300 units for ought to be *significantly* increased as accountability is fundamental to the development of trust required in the TDIF.

n. The penalty for contravening the prohibition on data profiling contained at s. 80(4) of the Bill of 300 units for ought to be *significantly* increased as accountability is fundamental to the development of trust required in the TDIF.

o. The penalty for contravening the prohibition on use of digital identity information contained at s. 81(3) of the Bill of 300 units for ought to be *significantly* increased as accountability is fundamental to the development of trust required in the TDIF.

p. The penalty for contravening the prohibition on use of data for marketing contained at s. 82(3) of the Bill of 300 units for ought to be *significantly* increased as accountability is fundamental to the development of trust required in the TDIF.

q. The penalty for contravening the prohibition retention of attributes and restricted attributes contained at s. 83(3) of the Bill of 300 units for ought to be *significantly* increased as accountability is fundamental to the development of trust required in the TDIF.

r. TDIF Trustmarks, as provided in ss. 84 and 85 of the Bill ought to be secured by and maintained as a registered certification trade mark pursuant to Part 16 of the *Trade Marks Act 1995* which would serve the purpose of ensuring that the TDIF Trustmarks have both the oversight of the Australian Competition and Consumer Commissioner and the transparency provided by the requirement that the Rules for Certification and publicly available. We additionally submit that the penalty of 200 units for misusing TDIF Trustmarks is insufficient and this penalty ought to be significantly increased to reflect the significant harm that may be caused by a person being misled to belief that information is being exchanged in a trusted environment.

s. The obligation at s. 132(2) of the Bill ought to be the destruction (and not the destruction or deidentification) of information) and the penalty of 200 units for failing to destroy information is insufficient and this penalty ought to be significantly increased.

15. We trust that this submission is of assistance.