HWL EBSWORTH
LAWYERS

Digital Transformation Agency

Privacy Impact Assessment Report

8 February 2022

Error! Unknown document property name.
Level 5, HWL Ebsworth Building, 6 National Circuit, Barton ACT 2600 Australia
PO Box 4316, Manuka ACT 2603 Australia
DX 5635 Canberra

Telephone +61 2 6151 2100
Facsimile 1300 769 828 (Australia) +61 2 8507 6583 (International)
hwlebsworth.com.au

1. Executive Summary

Introduction

1.1 The Digital Transformation Agency (**DTA**) has been tasked with expanding the Digital Identity System (**DI System**) by creating the Trusted Digital Identity legislation (**TDI Legislation**). The TDI Legislation consists of the Trusted Digital Identity Bill 2021 (**the Bill**), the TDIF Rules, and the TDIF Accreditation Rules. The DTA has commissioned a Privacy Impact Assessment (**PIA**) to examine potential privacy impacts of the TDI Legislation.

1.2 The draft TDI Legislation raises a range of potential privacy issues. We have identified throughout the body of the PIA where the DTA has already taken steps to address these issues, and the likely effectiveness of existing mitigation strategies for privacy impacts and risks. These questions have been addressed through headline issues which are then further analysed throughout the PIA report.

1.3 This report documents the process of the PIA and presents findings and recommendations for the DTA to consider.

Scope of this PIA

1.4 This PIA will consider privacy implications through an analysis of the privacy impacts and burdens created by the provisions of the draft TDI Legislation as drafted as at 21 September 2021.

1.5 This PIA will not consider:

(a) the compliance or otherwise of the TDI Legislation with the *Privacy Act 1988* (Cth) (**Privacy Act**) (see the Methodology section below);

(b) the privacy impacts of the Digital Identity System in which the TDI Legislation interacts; or

(c) the DTA's overall privacy practices.

Assumptions

1.6 This report relies upon a number of assumptions, including:

(a) that thorough consultation with appropriate agencies and departments has been conducted throughout the development of the TDI Legislation;

(b) from a policy perspective, privacy considerations have been balanced against policy objectives in consultation with relevant stakeholders;

(c) when the TDI Legislation comes into force and is implemented, additional privacy protections will be put in place as required (such as any required amendments to relevant agencies' privacy policies); and

(d) recommendations from previous PIAs conducted on the Digital Identity System have been adequately considered and, where appropriate, implemented.

Methodology

1.7 This PIA is undertaken in accordance with the process for undertaking a PIA recommended by the Office of the Australian Information Commissioner (**OAIC**) in its *Guide to Undertaking Privacy Impact Assessments*.

1.8 HWL Ebsworth Lawyers (**HWLE**) has prepared this PIA Report in consultation with the DTA. HWLE has relied on the DTA's source documents (listed at Schedule 1) for the description of the TDI Legislation and has drafted the analysis section of the PIA Report after receiving instructions from DTA that the description of the TDI Legislation in the first section of the PIA report accurately reflects the proposed handling of personal information.

1.9 The structure and analysis of this PIA is somewhat different to PIAs conducted in relation to a new system or policy being implemented by a government agency. That is because we have been provided with a draft Bill and sets of Rules to comment on before they are introduced into Parliament. Commenting on privacy issues and potential risks in relation to a piece of draft legislation will generally not involve assessing the Bill's compliance with the Privacy Act or the APPs. This is because the APPs expressly authorise, for example, the collection of sensitive information (APP 3.4(a)) and the use and disclosure of personal and sensitive information (APP 6.2(b)), if that collection, use, or disclosure is 'required or authorised' by an Australian law. To the extent that the Bill will require or authorise the collection, use or disclosure of personal and sensitive information, those activities will be compliant with the APPs and the Privacy Act by virtue of their being required or authorised by the legislation.

1.10 Accordingly, this PIA analyses the TDI Legislation's impacts on individuals' privacy and, where applicable, identifies and recommends options for avoiding, minimising or mitigating negative privacy impacts. It is focused on building privacy considerations into the design of the TDI Legislation. We do this by identifying the objectives of the Bill and the mechanisms that it uses to achieve those objectives. The mechanisms used by the Bill (eg civil and sometimes criminal penalties) to varying degrees impose a burden on individuals' right to privacy. We assess those privacy burdens and reach conclusions about the extent to which they are reasonable and proportionate to achieving the objectives of the Bill, and make recommendations for how any privacy risks can be mitigated.

1.11 On 14 October 2021 HWLE convened a meeting with instructors from the DTA in which DTA confirmed the scope of HWLE's instructions and approved the methodology set out above. In particular, DTA confirmed that this PIA report should assess the potential privacy risks and impacts of the draft TDI Legislation but not assess any risks or impacts arising from possible implementation strategies that may be implemented once the legislation comes into force. The scope of the PIA is to review the legislation and the rules. Additionally, DTA confirmed that this PIA would not recommend specific suggestions for amendments to the drafting of the TDI Legislation as this would be a matter for the drafting instructions provided to the Office of Parliamentary Counsel, which are currently being revised. The DTA also confirmed that HWLE is not required to consider the policy bases on which the TDI Legislation has been drafted, or the TDI system more generally. Other than being provided with the documents set out at Schedule 1 that describe the policy objectives that have informed the creation of the TDI Legislation, HWLE has not been instructed in relation to details of the policy choices that have been made in the course of the drafting of the TDI Legislation.

1.12 Accordingly, this PIA makes suggestions to mitigate privacy risks, however it does not propose particular language or suggested text for amendments to the TDI Legislation.

1.13 HWLE understands that the public consultation on the draft TDI legislation closed on 27 October 2021 and has not reviewed the consultation responses for the purposes of this PIA.

Progress of the matter

1.14 HWLE has worked in consultation with the DTA to identify headline issues for the DTA's consideration. On 22 July 2021, HWLE provided the DTA with initial comments on headline privacy issues following a high-level review of the draft Bill (a version marked 25 June 2021).

1.15 These identified headline issues were:

(a) community expectations;

(b) use of TDI Rules;

(c) penalty provisions; and

(d) use of digital identity information.

1.16 HWLE was provided with an amended version of the Bill on 21 September 2021 (the Exposure Draft version) and has updated the headline issues in this project description accordingly.

1.17 Notable changes include:

(a) Onboarding provisions (sections 21-29);

(b) Holding digital identity information outside Australia (section 31);

(c) Use and disclosure of personal information to conduct testing (section 38);

(d) Redress framework (sections 43-46);

(e) Notification of eligible data breaches (sections 67-69);

(f) Collecting and disclosing biometric information (sections 76-82); and

(g) TDIF Trustmarks (Chapter 5).

2. Recommendations

2.1 HWL Ebsworth Lawyers has made 3 recommendations in its assessment of the TDI Legislation. Those recommendations, and the responses to them, are as follows.

Recommendation 1.
Where there may be differences between the expectations of the community, determined from public consultation feedback, and provisions of the TDI Legislation, the DTA carefully assess what those differences may be and ensure that it has appropriate communication mechanisms in place to explain the rationale for the TDI Legislation to the Australian public.
Agency response

Recommendation 1.
DTA proposes to make a number of amendments to the exposure draft of the Bill based on the feedback and submissions on the draft Bill and rules. In addition, policy decisions and the preparation of the draft Bill (and draft legislative rules) have been informed by previous public and stakeholder consultation on proposed policy positions (see DTA's key public consultation documents *Digital Identity Legislation Consultation Paper* (November 2020) and *Have your say – Digital Identity Position Paper* (June 2021). Public and stakeholder feedback from those two consultation phases has been fed into policy consideration and decisions, including on the structure and detail of the exposure draft of the Bill and the draft rules. Noting that feedback on the exposure draft of the Bill not been uniform, policy decisions and justifications will be explained in the explanatory memorandum and associated materials on the DTA website.

Recommendation 2.
The DTA should conduct a review of measures currently contained in both sets of draft Rules, to determine the extent to which any of the measures contained in the draft Rules that have substantial privacy impacts could be drafted into the Bill instead of remaining in delegated legislation.
Agency response
The DTA, following public consultation and this PIA, will make the following changes. The Bill and draft TDIF accreditation rules will be amended in respect of accredited entities and disclosure of restricted attributes. The exposure draft of the Bill currently allows accredited entities operating within the trusted digital identity system (and which are authorised to disclose a restricted attribute of an individual) to disclose the restricted attributed to a participating relying party only if the participating relying party's conditions of onboarding authorise it to obtain the restricted attribute. However, for accredited entities operating in another digital identity system (**accredited-only entities**), the restriction on disclosure of restricted attributes is contained in the draft TDIF accreditation rules. This restriction for accredited-only entities will be lifted from the draft rules to the Bill. The new subclause will require that accredited-only entities not disclose a restricted attribute to a relying party unless the accredited entity's conditions of accreditation permit the disclosure to the relying party. Clause 19 of the exposure draft has been removed so that the Minister cannot make rules allowing entities to be taken to be approved to onboard to the trusted digital identity system. The most significant issues impacting on personal privacy have been included in the Bill (see, in particular, Chapter 2). The justification for leaving some requirements dealing with personal privacy in the legislative rules is the rapidly changing digital environment, which is subject to constant innovation as well as advancements to deal with digital fraud and cyber security matters. For example, many of the protective security requirements are likely to become outdated very quickly given the fluidity of technological advancements in the digital environment and emerging and complex risks. Maintaining such requirements in legislative rules facilitates rapid response while maintaining the need for public consultation, including where rules are made urgently (see clause 158) and parliamentary scrutiny (as required by the Legislation Act).

Recommendation 2.
The DTA, in consultation with the OAIC, Attorney-General's Department and stakeholders, will continue to closely review legislative rules as they are developed to ensure any matters that may impact personal privacy are appropriately placed in the legislative framework with detailed explanation on any privacy impacts and protections.

Recommendation 3.
If a proposed amendment to the Rules would have significant potential privacy impacts, the DTA consider implementing through the Bill a requirement that the OAIC be consulted on any such proposed amendment.
Agency response
DTA considers the following matters provide sufficient assurance of the Information Commissioner's involvement in any proposed amendments that would have significant potential privacy impacts. It is standard procedure for an agency with administrative responsibility for legislative changes to consult with other agencies where those agencies' responsibilities may be affected by the proposed legislative changes, or the other agency holds expertise in the subject-matter. Agencies must state in explanatory materials accompanying proposed legislative amendments who was consulted, including other agencies, on the proposed change (and faces criticism and questions by the relevant parliamentary committees if it has failed to consult). In addition, the Information Commissioner already has the functions of: • advising on matters relevant to the Privacy Act (noting that a breach or alleged breach of the additional privacy protections in the Bill are taken to be interferences with privacy under the Privacy Act) – section 28B(1)(a) of the Privacy Act; and • providing reports and recommendations to the Minister in relation to any matter concerning the need for, or the desirability of, legislative action in the interests of the privacy of individuals – section 28B(1)(c) of the Privacy Act. The Information Commissioner also has power to direct any agency to undertake a privacy impact assessment if the Commissioner considers that a proposed activity or function, including new or amended legislation or delegated legislation, might have a significant privacy impact – see section 33D of the Privacy Act and OAIC guidance at https://www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment As co-regulators under the Bill, the Oversight Authority and Information Commissioner will necessarily work closely together and co-operate on proposed recommendations for legislative changes to the policy agency with administrative responsibility for the Digital Identity Act when it commences. In addition, clause 158 of the Bill requires the Minister, who will make the legislative rules under clause 157, to consult on changes to those rules and consider any submissions made. This is in addition to the consultation requirement in section 17 of the Legislation Act.

3. Purpose of the TDI Legislation

3.1 The DTA created the DI System in order to modernise the way Australians and Australian businesses engage with government services by enabling Australians to verify their identity online. Currently, only services provided by Australian Government agencies can be accessed through the system.

3.2 The DTA is committed to expanding the system into the private sector and state, territory and local governments. To facilitate this expansion, the DTA is developing the TDI Legislation. The TDI Legislation is referenced at **Schedule 1**.

3.3 The draft Explanatory Memorandum provides that the purpose of the Bill is to:

(a) enable expansion of the DI system to state and territory governments and the private sector;

(b) formalise the appointment and the scope of powers for an Oversight Authority or authorities for the system to ensure it is run efficiently and is trusted;

(c) provide privacy protections, consumer safeguards and security requirements to build trust in the system;

(d) provide for a legally enforceable set of rules that sets the standards for participating in the trusted digital identity system (**TDI System**); and

(e) allow for entities to be TDIF accredited for their activities whether they are or are not on the system.

4. Overview of the TDI Legislation

4.1 The Bill broadly establishes three operational chapters relevant to this PIA:

(a) The TDI System (Chapter 2);

(b) The Oversight Authority (Chapter 6); and

(c) Accreditation (Chapter 3).

4.2 Chapter 2 establishes the TDI System itself. Chapter 6 provides for the roles and responsibilities of the Oversight Authority which is responsible for administering the TDI System, including undertaking fraud and cyber security investigations. Thirdly, Chapter 3 prescribes a process for accreditation, under which government entities and companies can apply for TDIF accreditation and undergo a series of assurance evaluations for their Digital Identity service. To become a TDIF accredited provider, applicants are required to demonstrate how their Digital Identity service meets a number of statutory requirements. Underpinning the system of accreditation are the TDI Accreditation Rules.

4.3 The Bill also prescribes privacy protections and administration provisions that apply to all of these operational systems.

4.4 It is important to note that the TDI Legislation is not intended to regulate the services provided by relying parties once an individual has verified their identity.

The TDI System

4.5 Section 14(1) of the Bill gives the Oversight Authority, established at chapter 6, the power to develop, operate and maintain a digital identity system.

4.6 Section 14(2) of the Bill states that a digital identity system established under section 14(1) is called the *trusted digital identity system*.

4.7 Under section 15 of the Bill, an entity may be onboarded to the TDI System as long as they are of the type listed in the table set out at this section and meet the corresponding criteria. These vary slightly between entities, but include that the entity must:

(a) be accredited (although this is not a requirement for an entity that is a 'relying party');

(b) hold approval under section 18 to onboard the system;

(c) if required by section 17 have a trusted provider agreement with the Commonwealth; and

(d) the onboarding day must have arrived or passed.

4.8 An entity is liable for 200 civil penalty units if they onboard in breach of the criteria set out at the table under section 15 of the Bill.

Oversight Authority

4.9 An interim Oversight Authority is responsible for the administration and oversight of the current DI system. This is intended to be replaced with the Oversight Authority created through the TDI Legislation.

4.10 Section 86 of the Bill establishes an Oversight Authority with the following functions set out at section 87:

(a) to identify and manage risks in relation to the TDI System;

(b) to manage the design of the TDI System and the process for coordinating outages, including to ensure that changes made by onboarded entities do not adversely affect the system as a whole;

(c) to determine service levels for accredited entities that hold an approval to onboard to the trusted digital identity system relating to the availability and performance of the entity's accredited facility;

(d) to determine service levels for participating relying parties relating to the availability and performance of each service the participating relying party is approved to provide, or provide access to;

(e) to establish and operate a test environment for the TDI System, and other electronic systems that interact directly with the TDI System, in accordance with the requirements (if any) specified in the TDI Rules;

(f) advise and assist entities in relation to their obligations under this Act;

(g) to promote compliance with this Act;

(h) to consult, cooperate with, and provide guidance to entities in relation to digital identity matters;

(i) to support, encourage, conduct and evaluate educational, promotional and community awareness programs that are relevant to digital identity matters;

(j) to advise the Minister, either on its own initiative or on request, on matters relating to any of the Oversight Authority's functions;

(k) to refer matters arising under this Act to the Australian Federal Police or the police force of a State or Territory;

(l) to facilitate, as required by law, access to information by law enforcement agencies (within the meaning of the *Australian Crime Commission Act 2002*) or any other agency or body of the Commonwealth, a State or a Territory;

(m) such other functions as are conferred on the Oversight Authority by or under this Act or any other law of the Commonwealth; and

(n) to do anything that is incidental or conducive to the performance of any of the above functions.

4.11 The Oversight Authority has broad powers in regard to these functions (section 88) and (other than the Minister's power to direct the Oversight Authority at section 20 to refuse to approve, or to suspend approval, for reasons of security) is not subject to direction by any person in relation to the performance or exercise of those functions or powers (section 89).

4.12 Further detail regarding the mechanics of the Oversight Authority are set out throughout chapter 6 of the Bill.

Accreditation

4.13 An entity can apply to the Oversight Authority to become an accredited entity, hence being able to onboard onto the TDI System in line with section 15. To do so an entity must first be granted authorisation to apply for accreditation by the Oversight Authority (section 48).

4.14 Only certain types of organisations will be granted authorisation under section 49 of the Bill. These are:

(a) an accredited attribute service provider;

(b) an accredited credential service provider;

(c) an accredited identity exchange;

(d) an accredited identity service provider; or

(e) an entity of a kind prescribed by the TDIF Accreditation Rules.

4.15 The Oversight Authority must also be satisfied, under section 48(1)(b) that:

(a) the facility through which the entity proposes to provide the services for which it will seek accreditation is sufficiently developed; and

(b) the entity has sufficient technical and financial resources available to it to become an accredited entity; and

(c) the entity has an adequate plan for progressing to accreditation as an accredited entity.

4.16 The Oversight Authority then decides whether to accredit an entity based on criteria set out at section 50 of the Bill.

4.17 Under the TDI Legislation, the Oversight Authority is granted rather broad powers to decide upon whether or not to accredit an entity. However, under section 50(5)(c) of the Bill, the Oversight Authority, when making a decision upon accreditation, must have regard to the matters (if any) prescribed by the TDIF Accreditation Rules.

4.18 The TDIF Accreditation Rules are further discussed at section 5 of this project description.

4.19 In summary, for an entity (other than relying parties), to apply to be part of the TDI System, the Oversight Authority must first grant them authority to apply for accreditation under section 48 of the Bill. They then must apply for accreditation to the Oversight Authority, having regard to the TDIF Legislation.

5. Trusted Digital Identity Framework Accreditation Rules

5.1 The DTA currently has a trusted digital identity framework which sets the standards, rules and guidelines for entities accredited or seeking to be accredited to participate in the DI System or another digital identity system. The purpose of the TDI Legislation is to make these rules enforceable for accredited entities.

5.2 The TDIF Accreditation Rules sit underneath the Bill. They apply for the purposes of the provisions of the Bill that authorise or require the TDIF Accreditation Rules to be made. The version of those Rules we have reviewed for this analysis is dated 17 September 2021.

5.3 Throughout the TDIF Accreditation Rules, different types of accredited entities are referred to by different letters. These are:

(a) “A” refers to an attribute service provider;

(b) “C” refers to a credential service provider;

(c) “I” refers to an identity service provider; and

(d) “X” refers to an identity exchange.

5.4 The TDIF Accreditation Rules expand upon the criteria which the Oversight Authority must consider when deciding whether to accredit an entity. Rule 1.1 outlines the matter which the Oversight Authority must have consideration to when making a decision on accreditation. These are:

(a) the level of the entity’s tolerance of digital identity fraud risk;

(b) the level of the entity's tolerance of cyber security risk;

(c) the content of, and the entity's ability to implement:

(i) its digital identity fraud control plan;

(ii) its privacy management plan;

(iii) its data breach response plan;

(iv) its system security plan;

(v) its disaster recovery and business continuity plan; and

(vi) its cryptographic key management plan;

(d) the results of the entity's usability testing under rule 5.6 of Chapter 4, as set out in the entity's usability test report;

(e) the results of the technical testing under Part 6 of Chapter 4, as set out in the entity's technical test report;

(f) the results of testing undertaken by the entity under rule 3.8 of Chapter 5, where such testing is applicable to the entity; and

(g) the findings of the functional assessments under Division 1, Part 7 of Chapter 4, as set out in the entity's functional assessment report.

5.5 The effectiveness of these criteria in ensuring the standard that accredited entities have to meet adequately protects personal information, will be assessed in this PIA.

5.6 The functional requirements for accreditation for each type of entity are set out at Chapter 4 of the TDIF Accreditation Rules and Chapter 5 outlines the role requirements of an entity once accredited. The effectiveness of these requirements will also be assessed in this PIA.

6. Trusted Digital Identity Rules

6.1 Trusted Digital Identity Rules (**TDI Rules**) also sit underneath the Bill. The version we have reviewed is dated 17 September 2021. The TDI Rules, made by the Minister for Employment, Workforce, Skills, Small and Family Business, expand upon the following provisions of the Bill:

(a) section 12 - Fit and proper person considerations;

(b) section 18(1)(g) - Applications for approval to onboard;

(c) section 22(7) - Conditions on approval to onboard;

(d) section 31 and 132(1) - Holding etc. digital identity information outside Australia;

(e) section 32(1) - Reportable incidents; and

(f) section 130(3) - Record keeping by onboarded entities and former onboarded entities.

6.2 Section 9(4) of the TDI Rules gives the Oversight Authority the power to grant an exemption to section 9(2) to allow an entity to hold digital identity information outside Australia. In doing so, section 9(5) provides that the Oversight Authority must consider any risk assessment plan provided by the entity, any PIA provided by the entity so far and the effectiveness of the entities protective security. The Oversight Authority may also consider whether any technology required by the entity is available in Australia.

6.3 Sections 10 to 18 of the TDI Rules require onboarded entities to report a number of privacy related breaches to the Oversight Authority, including, cyber security incidents (section 10), digital identity fraud incidents (section 11) and changes in use of trusted digital identity system (section 15). Details of these reportable incidents are able to be shared with other onboarded entities, the Oversight Authority and the Minister (section 17) and entities who experience a reportable incident must take reasonable steps to mitigate the adverse effects of the incident and eliminate or, if it cannot be eliminated, minimise, the risk of recurrence of similar incidents (section 18).

7. How the Bill interacts with the Privacy Act

7.1 As the TDI System is being established under legislation, it will operate in parallel with the Privacy Act by virtue of the fact that its measures will be legislated. Whatever the impacts on privacy are, it is likely that none will be impermissible as all will have the force of law, assuming that the TDI System is compliant with the Bill (and also provided that measures in delegated instruments are valid).

7.2 To the extent that a PIA would ordinarily consider compliance with the privacy law, that exercise would be a circular one where we consider the text of proposed legislation.

7.3 Part 2 of Chapter 4 of the Bill sets out how the legislation interacts with the Privacy Act. This includes extending the meaning of personal information (to the extent that the following terms are not covered by the Privacy Act definition of personal information) to explicitly include at section 64:

(a) attributes of individuals;

(b) restricted attributes of individuals; and

(c) biometric information of individuals.

7.4 Section 65 of the Bill establishes a prohibition on entities engaging in acts or practices with respect to personal information except in specified circumstances. Section 66 provides that contraventions of Div 2 of Pt 2 of Ch 4 of the Bill are interferences with privacy for the purposes of the Privacy Act. . An APP entity has the same meaning, as given in the Privacy Act, which is an agency or organisation as defined in section 6(1). A non-APP entity is not defined within the Bill or the Privacy Act and may need further clarification as part of this PIA.

7.5 Section 67 and 68 of the Bill prescribes that both APP and non-APP entities must make a notification to the Information Commissioner and the Oversight Authority if there is a suspected eligible data breach. Whether or not notification is sufficient to remedy eligible data breaches with be further discussed in this PIA.

7.6 Finally, various powers are granted to the Information Commissioner under the Bill (section 70) including the ability to disclose details of investigations to the Oversight Authority (section 71). This power is an additional function to those granted under the Privacy Act and will need to be examined to ensure it complements the Information Commissioner's existing powers under the Privacy Act.

8. Personal information flows

8.1 The Bill contemplates (although it does not explicitly create) certain information flows, chiefly between individuals, accredited entities, relying parties, the Oversight Authority and other organisations or other individuals such as the Australian Information Commissioner.

8.2 However, the Bill also establishes a complex and dynamic set of permissions and prohibitions on dealing with personal information in the sense that the Bill establishes a federated TDI system involving multiple layers and categories of actors who are each regulated differently. Accordingly, some of the movements of personal information are not readily captured by the concept of an information 'flow'. For instance, section 80 establishes a prohibition on data profiling, where digital identity information is held in the entity's accredited facility. That information may or may not include personal information. However, the prohibition does not apply in certain specified circumstances, including where the use or disclosure is for the purposes of providing the services for which the entity is accredited. While this may not be an information 'flow' created by the Bill, it is a prohibition on dealing with information (that may include personal information) subject to limited exceptions. This PIA report addresses these interlocking sets of prohibitions and permissions in the body of the PIA report.

8.3 In light of the above, we consider that the draft TDI Legislation contemplates the following circumstances in which personal information may be collected, used, and/or disclosed:

(a) accredited entities collect, use and disclose information about certain attributes of individuals, which may be subject to conditions imposed by the Oversight Authority under sections 22 and 23 of the Bill;

(b) accredited entities disclose a restricted attribute of an individual to a participating relying party in certain limited circumstances under section 74 of the Bill;

(c) accredited entities collect, use or disclose biometric information about an individual in certain limited circumstances provided for in sections 76 and 77 of the Bill;

(d) entities that are government entities are authorised to collect biometric information for other purposes, pursuant to section 78 of the Bill;

(e) an accredited entity may use or disclose personal information to conduct testing pursuant to section 38 of the Bill;

(f) an accredited entity may collect, use or disclose biometric information as provided for in Part 2, Division 2 of Chapter 4 of the Bill;

(g) personal information is collected by relevant entities, and then used and disclosed, in the course of responding to reportable incidents pursuant to section 32 of the Bill and sections 10-18 of the TDI Rules;

(h) personal information is collected by relevant entities, and then used and disclosed, in the course of taking required actions under the redress scheme provisions in Division 3 of Part 3 of Chapter 2 of the Bill;

(i) the Information Commissioner may disclose information to the Oversight Authority and State and Territory government agencies for the purposes of conducting investigations or performing other functions or powers, pursuant to sections 71 and 72;

(j) a person uses or discloses personal information for the purposes of performing functions under the Bill, or assisting in the administration or enforcement of another Australian law pursuant to section 104, or to a court or Tribunal pursuant to section 105; and

(k) relevant entities hold, store and/or handle digital identity information at a place outside Australia subject to the requirements of rule 9 of the Trusted Digital Identity Rules.

8.4 However, it is important to note that many of the flows of personal information contemplated by the draft TDI Legislation are likely to occur outside the purview of the legislation itself. In other words, the TDI Legislation establishes the overarching architecture or framework within which the TDI System will operate but does not prescribe each specific flow of information that will be required for the TDI System to operate. This PIA Report focuses on the TDI Legislation rather than the broader TDI System and accordingly there will necessarily be flows of personal information not captured in this analysis.

9. Analysis

9.1 There are a number of potential privacy issues which are raised by the draft TDI Legislation. This section of the report identifies privacy issues, analyses how the DTA can address these issues, and whether there are any outstanding concerns regarding the privacy impacts of the legislation that will need to be managed. This has been an iterative process involving consultation between HWLE and the DTA, and HWLE anticipates that it is possible that the legislation might undergo further changes during the process of, and following, this PIA.

Community expectations

9.2 The DTA has engaged in extensive public consultation which we consider is a privacy-positive step for the purposes of the draft TDI Legislation complying with the standards and expectations of the Australian community in relation to privacy.

9.3 The OAIC's guidance on conducting PIAs says that a PIA should go 'beyond compliance to also consider the broader privacy implications and risks, including whether the planned uses of personal information in the project will be acceptable to the community.' In reference to the TDI Legislation, where compliance with the Privacy Act is not in issue, we think that community expectations therefore become more important.

9.4 The DTA has conducted public consultation in three phases:

(a) Phase 1 - consultation paper (16 November 2020 - 18 December 2020)

(b) Phase 2 - position paper (10 June 2021- 14 July 2021)

(c) Phase 3 - exposure draft legislation (1 October 2021- 27 October 2021)

9.5 This PIA assesses the privacy impacts of the TDI legislation against submissions made under phases 1 and 2, alongside public sentiment as assessed in the *Australian Community Attitudes to Privacy Survey 2020*,[1] conducted by the OAIC.

Phase 1

9.6 In response to Phase 1 consultation on the TDI consultation paper, the OAIC made a submission containing two recommendations:

(a) Privacy protections should be contained in primary legislation, rather than subordinate instruments such as the Operating Rules.

(b) The legislation should explicitly limit the collection, use, and disclosure of personal information to specific purposes.

9.7 The submission from the eSafety Commissioner stated that age and identity validation, verification and authentication have attracted increased attention as potential technological measures to assist in addressing and preventing some forms of online harm amongst the online safety community in recent years. eSafety's research and experience points to the fact that the general public want greater control over, trust in, and more transparency from, the digital technologies and systems that they use.

9.8 The Australian Communications Consumer Action Network's (**ACCAN**) submission recommended that the definition of Digital Identity should be harmonised with the Privacy Act to create a robust network of privacy protections for consumers. ACCAN also submitted in response to the Attorney General's Department Privacy Act Review Issues Paper that the current definition of personal information and sensitive information in the Privacy Act needs to be expanded to suit modern data collection practices.

9.9 PwC submitted a submission which stated that PwC Australia's recent Citizen Survey 2020 reported a fundamental shift in the public's use of digital channels to access Government services and a significant increase in public trust for the Australian Government as a result of responses to the National Bushfires and COVID-19 pandemic. The Citizen Survey conducted by PwC whilst reporting an overall increase in public trust towards the Australian Government, found the majority of citizens still remain generally neutral in their feelings of trust towards government. From these submissions it is evident that ensuring privacy by design will be critical to securing public trust and confidence in the Digital Identity system.

Phase 2

9.10 The Australian Information Security Association recommends ensuring that the use of Digital Identities created and managed through the TDIF system is voluntary, and alternatives continue to exist in perpetuity which are still "usable" and "accessible" by Australians and deliver the same level of access. It is important to ensure Australians are not coerced to use TDIF systems.

9.11 The Queensland Council for Civil Liberties submitted that a person ought to be able to:

(a) by default, opt out of the creation of a digital identity;

[1] https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey

(b) alter or amend their digital identity; and

(c) at any stage, require that their digital identity be deleted (in a similar manner to the "right to be forgotten").

9.12 The Queensland Council for Civil Liberties also submitted that the Oversight Authority and its Advisory Boards ought to be responsible for the integrity of the system rather than the utility of the system and the Legislation ought to include provisions where a Participant will be "offboarded" as a consequence of an adverse finding of the Information Commissioner and where the Participant is found to have offended any 'privacy law' where that term is defined broadly to include any statutory or common law obligation.

Australian Community Attitudes to Privacy Survey 2020 (OAIC) [2]

9.13 OAIC conducted a survey in 2020 regarding community attitudes to privacy. The survey found that Australians' level of comfort with certain data practices depends on the type of information collected, the purpose behind it, and the level of trust in the organisation involved. Australians appear more comfortable with data practices where the purpose is clearly understood – for example, law enforcement using facial recognition and video surveillance to identify suspects

9.14 However, Australians are concerned about businesses tracking individuals' location through mobiles or web browsers (62%) and are generally reluctant to provide biometric information (66%). Commercial profiling activities drive higher levels of discomfort than government data practices.

9.15 In addition the survey made the following findings:

(a) Australians believe that the biggest privacy risks facing the community are online services, including ID fraud and theft, data security breaches, and social media sites.

(b) Health service providers are the most trusted organisations with regard to how they protect Australians' personal information during the COVID-19 outbreak (72% trustworthy), followed by their employer (64% trustworthy) and Federal Government agencies (54% trustworthy).

(c) The Australian Government is generally more trusted than businesses with the protection of personal information. Certain purposes are considered more legitimate than others, such as public safety. Australians are slightly more comfortable with most instances of government use of personal information than they were in 2017.

(d) 'Australians are more likely to be comfortable (36%) with government agencies sharing information with other government agencies now, compared with 30% in 2017. Similarly, the proportion of people who are uncomfortable with this practice (40% in 2020) has decreased since 2017 (45%)'.

(e) Among the most likely practices to be considered a misuse of personal information (84%) is an organisation using personal information in ways that cause harm, loss or distress More than 4 in 5 Australians (84%) consider supplying information to an organisation for a specific purpose and the organisation using it for another purpose to be misuse.

[2] https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey

9.16 While there has been a decrease in trust in organisations to handle personal information, the survey points to other factors that increase trust and transparency, such as certification.

9.17 Community attitudes to privacy need to be balanced with the statutory objects of the TDI legislation. We note that the objects of the Bill are outlined in s 3 as being:

(a) to provide individuals with a simple and convenient method for verifying their identity in online transactions with government and businesses, while protecting their privacy and the security of their personal information;

(b) to promote economic advancement by building trust in digital identity services;

(c) to facilitate economic benefits for, and reduce burdens on, the Australian economy by encouraging the use of digital identities, online services and the interoperability of systems using digital identities;

(d) to provide a digital identity system that will enable innovative digital sectors of the Australian economy to flourish.

9.18 As set out in the methodology section of this PIA, community expectations can be used to consider specific issues surrounding privacy which arise from the TDI Legislation, rather than assessing the TDI Legislation specifically against the Privacy Act. Where there may be differences between the expectations of the community, determined from public consultation feedback, and provisions of the TDI Legislation, **we recommend (Recommendation 1)** the DTA should carefully assess what those differences may be and ensure that it has appropriate communication mechanisms in place to explain the rationale for the TDI Legislation to the Australian public, having regard to the objects of the Bill and the policy rationale for the TDI system.

Privacy safeguards

9.19 Division 2 of Part 2 of the Bill steps out additional privacy safeguards on top of compliance with the Privacy Act.

9.20 These additional safeguards include:

(a) Extending the definition of personal information (section 64);

(b) Restrictions on disclosure of attributes of individuals to relying parties (section 73);

(c) Prohibition on single identifiers (section 75);

(d) Restrictions on collecting, using, disclosing and deleting biometric information (sections 76-79);

(e) Prohibition on data profiling (section 80);

(f) Prohibited enforcement purposes (section 81); and

(g) Prohibited marketing purposes (section 82).

9.21 Breaches of certain of these provisions of the Bill result in a civil penalty of 300 penalty units for entities operating within the TDI System.

9.22 Our view is that, generally speaking, the privacy safeguards outlined in the Bill are privacy positive, and that they significantly advance the extent to which personal information is protected through the TDI scheme. By way of example, we note that section 64 of the Bill expands the definition of 'personal information' to include the type of personal information obtained under the Bill, such as personal information about the attributes of individuals, restricted attributes of individuals and biometric information of individuals – this is broader than the definition of personal information in the Privacy Act, and means that the requirements in the Privacy Act about collecting, using and disclosing personal information under that Act extend to information of the kind set out in section 64 such that the attributes of individuals, restricted attributes of individuals, and biometric information of individuals collected under the TDI System will be protected.

9.23 There are several other significant features of the TDI Legislation which in our view balance the potential privacy issues with the expectations of the Australian community with respect to privacy, as follows:

(a) The voluntary nature of creating a digital identity, provided for in section 30. In order to access services that are part of the TDI system, a person will not be required to create a digital identity, and there is a prohibition (subject to exceptions) on requiring an individual to generate or use a digital identity as a condition of providing a service or access to a service.

(b) The Bill seeks to ensure that where possible individuals are given the opportunity to consent to the handling of their personal information, including prior to the disclosure of an attribute of the individual to a relying party (section 73), disclosure of a restricted attribute of the individual to a relying party (section 74), and also prior to the collection, use or disclosure of biometric information (section 76(1)).

(c) Once a person creates a digital identity, section 61 provides that the relevant accredited identity service provider must, if requested to do so by the individual, deactivate the digital identity of the individual as soon as practicable after receiving the request.

9.24 We consider that these additional safeguards are privacy positive and would be consistent with the community's expectations for the protection of individual privacy.

Use of TDI Rules

9.25 One potential area of concern from a privacy perspective is that some of the privacy protections will be determined by TDI Rules and not inserted into the Bill. This means that certain important privacy-related concepts and protections in the TDI system would be at the discretion of the Minister, and subject to a lesser degree of parliamentary scrutiny than if the provisions were inserted into the Bill itself.

9.26 Examples of where the TDI Rules appear to deal with measures (or are empowered to deal with measures) that may impact privacy include:

(a) approval to onboard to the system (see section 19 of the Bill and sections 5-7 of the TDI Rules)

(b) conditions on approval to onboard to the system (see section 20 of the Bill and section 8 of the TDI Rules);

(c) security reliability and stability requirements to onboard to the TDI System (see section 22(3) of the Bill);

(d) voluntary generation of a digital identity (see section 30(2)(c) of the Bill);

(e) holding digital identity information outside Australia (section 31(1) of the Bill and section 9 of the TDI Rules);

(f) reportable incidents (see section 32(1) of the Bill and sections 10-18 of the TDI Rules); and

(g) redress obligations (see section 45 of the Bill).

9.27 Our view is that some of these measures, and the different way measures are expressed in the TDI Rules, will have varying impacts on privacy. Holding digital identity information outside Australia is likely to have the greatest potential impact on privacy, along with the disclosure of personal information without the need for the individual's consent in response to a reportable incident. The balance of these measures we assess as having a relatively low impact on privacy, while measures including the voluntary nature of creating a digital identity and security reliability and stability requirements are privacy positive.

9.28 Our assessment is that it is reasonable to expect that the Australian public would, as a general proposition, consider that legislative measures with significant privacy impacts should be contained in primary legislation as opposed to delegated legislation, in circumstances where primary legislation is subject to a greater degree of parliamentary scrutiny before being passed into law. Accordingly, we **recommend (Recommendation 2)** that the DTA conduct a review of measures currently contained in both sets of draft Rules, to determine the extent to which any of the measures contained in the draft Rules that have substantial privacy impacts could be drafted into the Bill.

9.29 In circumstances where the Bill provides broad powers for aspects of the TDI System to be enacted through the TDI Rules, we also **recommend (Recommendation 3)** that if a proposed amendment to the Rules would have significant potential privacy impacts, the DTA consider implementing through the Bill a requirement that the OAIC be consulted on any such proposed amendment.

Holding digital identity information outside Australia

9.30 There may be privacy concerns with the ability of entities to hold, store, handle or transfer digital identity information outside Australia.

9.31 Section 31 of the Bill provides that the TDI Rules may make provision in relation to the holding, storing, handling or transfer of digital identity information outside Australia if the information is or was generated, collected, held or stored by accredited entities within the trusted digital identity system. Section 9 of the TDI Rules then creates a set of permissions and requirements for entities and the circumstances in which they may hold, store, handle or transfer digital identity information outside Australia. Simply put, an entity must not transfer or hold digital identity information outside Australia, unless it has applied for and been granted an exemption by the Oversight Authority pursuant to s 9(4) of the TDI Rules.

9.32 There could be potential community privacy concerns with the holding of digital identity information outside Australia, and whether the provisions of section 9 of the TDI Rules adequately address these potential concerns.

9.33 There are a number of community expectations which need to be considered, when deciding how to handle and store information outside Australia. Based on stakeholder submissions to

the DTA's consultation processes, there appears to be a clear preference for Australian government agencies to hold information as opposed to private entities and organisations. Particularly following the Covid-19 pandemic, the PwC Citizen Survey 2020 found that trust in Government has increased whilst the *Australian Community Attitudes to Privacy Survey 2020 (OAIC)* found a decrease in trust in non-government organisations to handle personal information.

9.34 Although we have not been instructed to review the underlying policy documents, it is reasonable to assume that there is a practical imperative behind the authorisation for entities to transfer and hold information that includes personal information outside Australia. This practical imperative needs to be balanced against the potential public perception that offshore storage of personal information – particularly if it is stored by private entities which appear to be trusted less than government agencies – has greater possibility of adverse consequences than storage of personal information in Australia.

9.35 Noting that one of the objects of the Bill is to provide individuals with a simple, convenient and secure method for verifying their identity in online transactions (see section 3), our view is that it is reasonable to conclude that the Australian community would accept a system for transferring and holding personal information outside Australia that is regulated by the Oversight Authority in the manner provided for in section 9 of the TDI Rules.

Reportable incident measures

9.36 There could be potential privacy concerns with the TDI Legislation's framework for dealing with reportable incidents, and the circumstances in which personal information may be used and disclosed in the course of responding to such an incident. In relation to reportable incidents, we note that TDIS operates as a federated system, which by design requires participants to share information to prevent, address and track cyber security and fraud incidents.

9.37 Section 32 of the Bill provides that the TDI Rules may prescribe arrangements relating to the notification and management of reportable incidents. Sections 10-18 of the TDI Rules then make provisions for the kinds of reportable incidents in respect of which entities have reporting obligations. By way of example, section 10 of the TDI Rules provides that entities must notify the Oversight Authority in the event of a cyber security incident, and also notify the Oversight Authority of a digital identity fraud incident pursuant to section 11 of the TDI Rules. Section 17 provides that the Oversight Authority may disclose information notified to it about a cyber security incident, to an onboarded entity, the Minister, or an enforcement body. Information relating to a cyber security incident is likely to include personal information of affected individuals.

9.38 We note that, to the extent that information about an incident contains personal information, the authorisation to disclose information pursuant to section 17 of the TDI Rules does not require that the Oversight Authority seek the consent of the person to whom the information relates prior to disclosing it. The draft Statement of Compatibility with Human Rights for the TDI Legislation notes, at [6.4] that:

> *It is noted that instances may arise where, in implementing the digital identity system provided under the Bill, personal information may be disclosed, without consent in the management of investigations of identity fraud and cyber security incidents. This is a narrow exception to the requirement for consent put in place because an entity has the responsibility to prevent, detect and deal with cyber security risks and digital identity fraud in the proposed TDIF Accreditation Rules. This has the effect of limiting the right to privacy. To ensure this limitation is reasonable and not arbitrary, mechanisms that are put in place to regarding these types of incidents and protective*

measures will be implemented under the rules. The proposed rules will contain the specific mechanisms and procedures relating to incidents of fraud or threats to cyber security, including measures relating to incident management, investigations, reporting system security and digital identity fraud control plans.

9.39 Our view is that the ability to disclose personal information without consent following a reportable incident represents a burden on the privacy of individuals as it is an exception to the TDI Legislation's emphasis on consent. However, in circumstances where disclosure of personal information without consent is to be undertaken in the course of responding to threats such as digital identity fraud and cyber security incidents, this is likely to represent a proportionate response to the threats posed to individuals by such incidents, which could be significant. We recognise that if the Bill were to require entities to seek the consent of potentially affected individuals following a reportable incident, this could significantly hamper efforts to respond to incidents effectively.

Redress framework measures

9.40 There may be privacy concerns with the ability or otherwise of accredited entities to prevent and respond to digital identity fraud incidents and other cyber security incidents, although we consider that these measures are reasonable and proportionate to the legislative objective of minimising harm to individuals who participate in the TDI System.

9.41 Division 3 of Part 3 of Chapter 2 of the Bill establishes a 'redress framework' setting out the actions that accredited entities must take in the event of digital identity fraud incidents and cyber security incidents, including informing affected individuals and businesses, and informing the Oversight Authority. It also prescribes measures that accredited entities must take to avoid such incidents, such as maintaining policies to deal with incidents (section 43(5)). It is likely that personal information will be collected, used and disclosed in the course of taking actions required by the redress framework provisions.

9.42 In relation to redress framework, we note that first, the obligations of entities are engaged when there has been a cyber security or fraud incident. Furthermore, the accredited entities are likely to already have the affected individual's business's contact details (as the individual is likely to have a digital identity). It can be reasonably assumed that most individuals who are affected by cyber and fraud incidents would want to be advised so they can take appropriate actions to protect themselves (e.g. notify their banks, etc.). Accordingly, although the redress framework will likely involve the collection, use and disclosure of personal information we assess the framework as largely privacy neutral.

Conditions relating to the collection and disclosure of information about individuals

9.43 A further potential privacy issue arises from the way in which the TDI Legislation provides that entities may use or disclose personal information about individuals, and what is defined as 'restricted attributes' such as health information about the individual (which is sensitive information for the purposes of the Privacy Act). The Oversight Authority has power to grant permission to entities to collect and disclose restricted attributes of individuals, and the ability to impose limitations on that power to collect and disclose. However, we note that the Bill proposes a layered framework of protections that is designed to prevent this information being treated in a way that would be an unlawful or arbitrary infringement of privacy.

9.44 When the Oversight Authority gives approval for an entity to onboard to the trusted digital identity system, it may place conditions on the kinds of attributes of individuals that the entity is authorised to obtain or disclose and the circumstances in which such attributes may be obtained or disclosed and the kinds of restricted attributes of individuals (if any) that the entity is

authorised to obtain or disclose and the circumstances in which such attributes may be obtained or disclosed (section 22(6)). Section 22(6) confers a discretion on the Oversight Authority to authorise the kinds of restricted attributes of individuals that entities are in turn authorised to obtain or disclose and the circumstances in which such attributes may be obtained or disclosed. The Explanatory Memorandum to the Bill provides that restricted attributes need 'to be managed with special care because of the sensitivity of some the information which may be involved'.

9.45 Under section 23, the Oversight Authority must have regard to certain matters before it grants such a permission to obtain or disclose information about restricted attributes, including the potential harm that could result if restricted attributes of that kind were disclosed to an entity that was not authorised to obtain them, community expectations as to whether restricted attributes of that kind should be handled more securely than other kinds of attributes, and whether disclosure of restricted attributes of that kind is regulated by another law of the Commonwealth. Participating relying parties must have authorisation from the Oversight Authority before they can receive restricted attributes, pursuant to section 74(2).

9.46 Our view is that the safeguards provided for in section 23 are probably consistent with community expectations in relation to the circumstances in which entities should be permitted to use or disclose personal information about individuals, and particularly 'restricted attributes' of individuals, because it imposes appropriate limitations that are to some degree at the discretion of the Oversight Authority and accordingly can be tailored to particular circumstances.

Section 19 - Entities may be taken to be approved to onboard to the trusted digital identity system

9.47 The approach the DTA has taken to delegating the ability for onboarding to the TDI Rules, is to allow the option for self-service onboarding to occur in the future. Section 19 of the Bill provides that entities may be taken to be approved to onboard to the trusted digital identity system, and that this may be provided for in the TDI Rules.[3]

9.48 This approach is to be balanced against the potential privacy impacts of not specifying the onboarding provisions TDI legislation.

The Oversight Authority and the OAIC – overlapping regulatory roles

9.49 In phase 1 of public consultations, the OAIC submitted a recommendation that:

> *'The OAIC is designated as the Oversight Authority for the privacy aspects of the system.'*

9.50 In phase 2 of consultations, the OAIC submitted two recommendations in regard to its power under the TDI Legislation, including:

> *Recommendation 1: The DI legislation should provide the Information Commissioner with comprehensive regulatory functions and powers, drawing on existing regulatory functions and powers under the Privacy Act to the extent possible.*
>
> *Recommendation 2: The Information Commissioner should be empowered to issue infringement notices for breach of the new privacy protections under the DI legislation.*

[3] We note that the DTA has subsequently advised that s 19 will be deleted from later versions of the TDI Bill.

9.51 It appears similar issues have been raised about the proper regulatory agency to enforce certain provisions of the Bill during further consultations with the DTA about the identity of the Oversight Authority and the performance of other regulatory functions. Based on the material we have reviewed, the Attorney-General's Department recommended:

(a) In relation to section 73 of the Bill, which imposes a civil penalty if an accredited entity which is operating within the trusted digital identity system discloses an attribute of an individual to a relying party without the express consent of the individual:

> *'If the OAIC is intended to regulate this provision, AGD's preference is rather than making the provisions civil penalty provisions, they should constitute an interference with privacy and therefore trigger the OAIC's usual enforcement powers and actions under the Privacy Act. This has the benefit of ensuring that if the Privacy Act is uplifted as a result of the current Review, the enforcement mechanisms will automatically be uplifted in relation to the Digital Identity System.*
>
> *If DTA is of the view that these provisions are significant enough that they need to be subject to a civil penalty, AGD strongly prefers that no infringement notice therefore apply to a civil penalty of this nature and instead for the civil penalty instead to apply. This is similar to the My Health Record system as we understand it.'*

9.52 We note that in the version of the Bill we have reviewed, the civil penalty in s 73 would apply to onboarded accredited entities for certain conduct only. Section 66 of the Bill provides that conduct which contravenes Div of Pt 2 of Pt 2 of Ch 4 is an interference with privacy for the purposes of the *Privacy Act*, and this would trigger the OAIC's enforcement powers and actions under the *Privacy Act* for a contravention of s 73 of the Bill.

9.53 Similarly, in relation to s 66 of the Bill which provides that contraventions of Division 2 of the Bill are interferences with privacy for the purposes of the Privacy Act, AGD submitted that:

> *As a general comment we note the proposed framework whereby a state and territory agency will be regulated by the OA, their own state/territory privacy regulator AND the OAIC in relation to the additional privacy protections, is a very confusing regulatory model. However we understand the states/territories are unwilling to have the OAIC regulate all privacy aspects.*

9.54 In relation to section 120 of the Bill, which establishes a regime of infringement notices in relation to civil penalty provisions and provides that the Oversight Authority is the infringement officer for each civil penalty provision in the Bill, OAIC made the following submission:

> *… we recommend that the Information Commissioner is directly empowered to issue infringement notices in relation to the relevant additional privacy protections under the Digital Identity legislation. We consider the Information Commissioner or a member of staff of the Commissioner who is equivalent to a SES employee should be an infringement officer and the Information Commissioner should be the relevant chief executive. We understand that this is an issue that AGD wishes to discuss further, but we would be grateful if you could provide any feedback from OPC as to whether there are any drafting or legal impediments to taking this approach.*

9.55 We note that the Bill has subsequently been amended and that DTA considers the issue of infringement notices to be resolved.

9.56 The DTA have stated that it will monitor amendments to the Privacy Act that could affect the issuing of infringement notices, and can consider amending this provision if OAIC is given these powers as part of that review. Our view is that there may be residual privacy concerns with the potentially overlapping regulatory roles of the Oversight Authority and the OAIC, with State and Territory privacy regulators also having some responsibilities in relation to entities that are State or Territory government agencies. In short, entities and individuals may perceive a lack of transparency in the TDI Legislation if it is difficult to discern who the relevant regulator is for a particular aspect of the legislation. Both the Attorney-General's Department and the OAIC have made submissions in relation to the allocation of regulatory roles for the enforcement of provisions in the Bill, and at this stage it appears that the issues raised by those submissions remain unresolved.

Schedule 1: Source Documents

Source Documents
Trusted Digital Identity Bill 2021- B21PX116.V27 (Draft dated 17 September 2021, Exposure Draft version)
TDI Rules (Draft dated 17 September 2021)
TDIF Accreditation Rules (Draft dated 17 September 2021)
Digital Identity- Guide to DI Legislation (dated 17 September 2021)
Digital Identity Legislation Consultation Background Paper_131120_0930 (for consultation 16 November and 18 December 2020)
Digital Identity Legislation Position Paper Final (for consultation 10 June and 14 July 2021)
Explanatory Memorandum for the Trusted Digital Identity Bill 2021 (Draft dated 18 October 2021)
Internal DTA email correspondence Re: S 19 - RP taken to be onboarded - further consideration
DTA DRAFT Statement of Compatibility with Human Rights for the TDI Bill (Draft dated 14 October 2021)