Digital Identity Legislation Consultation Paper

PwC Submission

December 2020

Table of contents

1. Executive summary

Our view on the development of Digital Identity legislation

Securing the future economic prosperity of Australia

Over the last decade, businesses and Government have become increasingly reliant on digital information, and Digital Identity has become a fundamental building block to effectively operate and compete in a digitally connected world. Following the Financial Systems Inquiry, the Trusted Digital Identity Framework (TDIF) was established and has provided the rules and accreditation criteria that providers of Digital Identity services are accredited against; thereby creating a federation of agencies and systems working together to deliver an Australian Digital Identity system.

The TDIF has been successful in shaping how Australia provides Digital Identity services and through its use over the past three years has shaped the way the Government has responded in this area. The rapid growth of Digital Identity needs, which has been exacerbated by the COVID-19 pandemic, has demonstrated that as a country we are starting to outgrow the current iteration of the framework and surrounding legislation. Over this time, the evolution of the TDIF framework has demonstrated the increased maturity of Australian citizens and entities to move towards a more holistic Digital Identity system that could be expanded to include international or border and customs use cases similar to that seen in Luxemburg and other parts of Europe.

An enhanced legislative framework for the Digital Identity system is needed to facilitate an expansion of the current model for new use cases and greater adoption in the private and public sector. The development of Digital Identity legislation will allow the Government and participants to build a system to support Australian citizens now and into the future.

A limitation of the current TDIF is that it is quite prescriptive; being able to separate out different elements into primary legislation, legislative instruments and policy is a big advantage to 'future proofing' the system.

PwC Australia's recent Citizen Survey 2020[1] 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 Government as a result of responses to the National Bushfires and COVID-19 pandemic. When the pandemic first

[1]https://www.pwc.com.au/consulting/customer-led-growth/citizen-survey.html?icid=CitizenSurvey2020-social-staff-organic-staffsocshare

struck Australia, government workforces mobilised at unprecedented speed and scale to expand services and provide additional support for citizens.
This included relaxing identity set-up requirements in the short term so that citizens could get quicker access to essential JobKeeper payments[2].

The need to create a safe and secure Digital Identity system is not an issue unique to Australia and we have seen other countries embark on this challenge. Canada and New Zealand are currently at a similar position to Australia, however, other countries, such as the UK, Belgium, and Singapore are further progressed, providing us with an opportunity to observe and learn from their experiences.

As one of Australia's leading professional services firms, with touch points across the Digital Trust system, PwC believes that we have unique perspectives that we can share on these important issues. This submission paper includes our points of view and responses to questions posed in the consultation paper which we feel we are well positioned to contribute to, based on our experience and insights from both clients and colleagues across our global network.

[2]https://www.pwc.com.au/consulting/citizencentric/pwc-australia-citizen-centric-report-2020.pdf

2. Overview of the legislation

Why is the legislation needed?

The rapid shift in the public's adoption of digital channels to access Government services using secure and trusted methods could not be more relevant than now in response to the COVID-19 lockdown restrictions[3]. The Digital Identity system has become a key channel in which the public uses government services and secure methods of proving and providing identity information is a critical component of this rollout of services.

The Digital Identity program known as the Digital Identity System is used by over 1.7 million Australians and 1.2 million businesses to access over 70 Government services. With ever increasing growth in the adoption of digital services, it has become clear that additional governance in the form of overarching legislation is required to establish permanent oversight and governance structures for the system and to build public trust of Government and private Sector digital services.

The TDIF currently includes a range of system specific privacy and consumer protections for users, such as:

- Restrictions on the creation and use of a single identifier across the system
- Restrictions on data profiling
- Restrictions on the collection and use of Biometric Information
- Requiring express consent before enabling User authentication to a service

However, these requirements are not currently enshrined in law and may be subject to changes according to the policies of the day.

Embedding these requirements as legislative provisions so that they become subject to the checks and balances of parliamentary processes and have robust legal enforcement mechanisms, will help build public trust in the Digital Identity system.

Privacy is a major concern to the Australian community. Identity theft and fraud were the most significant privacy concerns identified by 76 per cent of respondents to the Office of the Australian Information Commissioner 2020 Australian Community Attitudes to Privacy Survey.[4] Previous attempts to build community support for Government management of personal information (such as the My Health Record system and the COVIDSafe app) have demonstrated a degree of anxiety in the Australian community about the controls that exist to ensure personal information is used and disclosed appropriately and transparently.

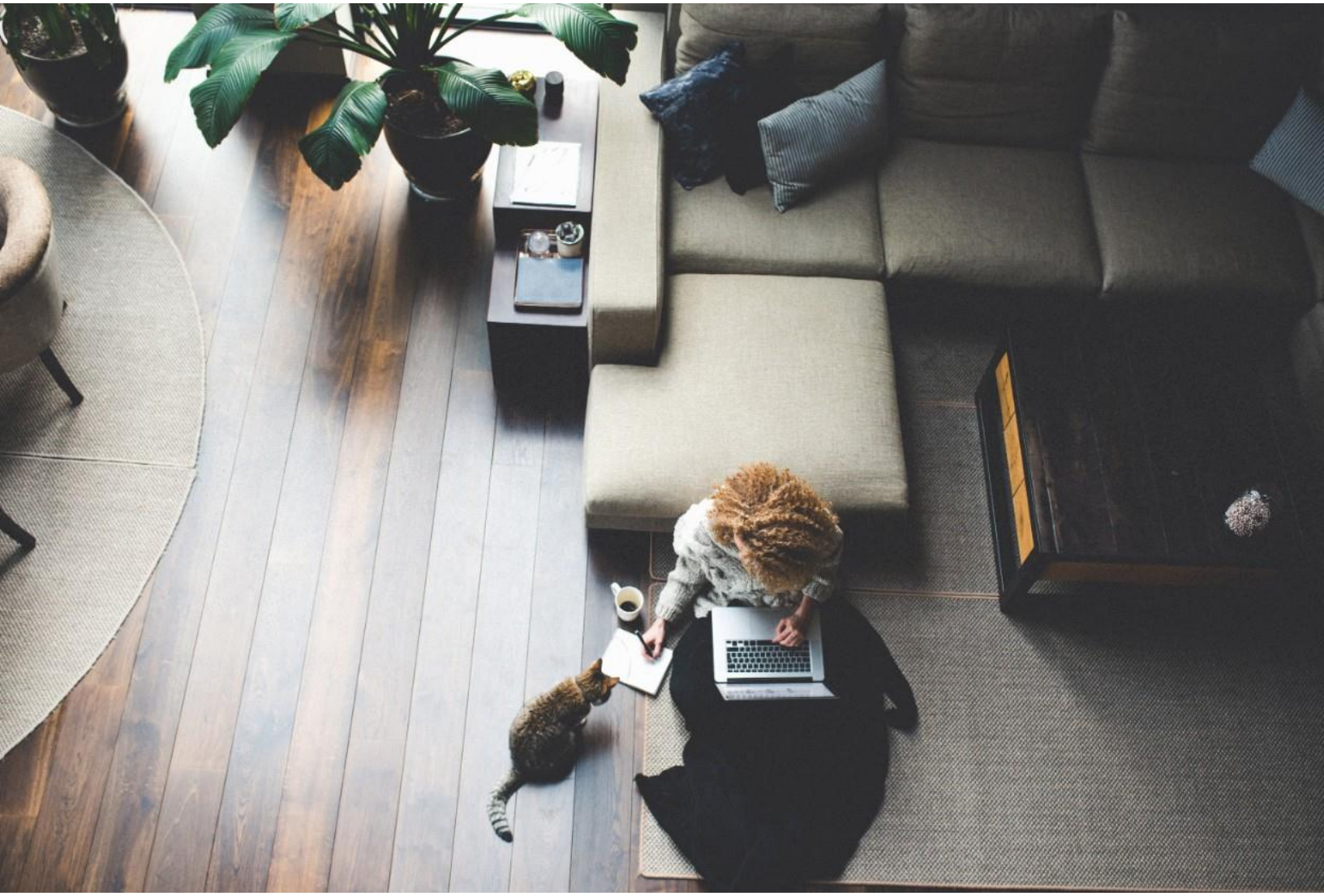
As highlighted earlier, the recent Citizen Survey conducted by PwC whilst reporting an overall increase in public trust towards the Government, found the majority of citizens still remain generally neutral in their feelings of trust

[3] 37% of respondents say their use of digital channels has increased during the COVID-19 pandemic https://www.pwc.com.au/consulting/citizencentric/pwc-australia-citizen-centric-report-2020.pdf - page 3

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

towards Government[5]. Securing the public's trust in the Digital Identity system will be critical to the success of the policy which is the enshrining of principles governing security and privacy in law is important to reassure the public that safeguards have been considered, cannot be easily amended and can be appropriately enforced.

Similarly, provisions granting authority to an oversight body and enforcement powers will need legislative force to be able to operate effectively.



[5] https://www.digitalpulse.pwc.com.au/citizen-government-trust-experience/

How it should be structured

Given the pace at which technology moves and changes, the nature of legislation can be somewhat inflexible. To this end, there needs to be careful consideration of what rules and requirements are best suited to technical standards, delegated rules or enshrined in legislation.

We have outlined above some of the elements which could be factored into the legislation. Operating rules and other legislative instruments will be important to address areas which will be subject to more frequent changes, i.e., technology, security, fraud, data and privacy elements. We only need to look to the events of the past year, in response to the COVID-19 pandemic, to understand the need for flexibility and agility in order to be able to respond to emergency situations. The public's rapid change in the way in which they interact with Government services will require strong and agile measures to react.

Operating rules can be amended by the responsible Minister and are a better option for public or private cooperation as they can be revised more easily, similar to technical standards, and are therefore better able to adapt to rapid technology change. Similarly, for these reasons, prescriptive technical specifications are best located in policy frameworks.

Identity proofing considerations

While the guidance on assurance levels has come a long way in the most recent iterations of the TDIF, there remains a number of areas for review and additional safeguards to be implemented. Release 4 of the TDIF has taken further steps to account for Private Sector concerns by developing additional proofing levels that align with Know your Customer (KYC) requirements.

Identity Proofing thresholds for accessing a relying party's services should be mediated by both an understanding of the inherent risk of that transaction as well as an assessment of the risk from a Digital Identity system-wide perspective.

The potential need for prescriptive controls should be balanced with the need for adaptive fraud mitigation strategies for the whole ecosystem to manage potential fraud that may occur with these high risk transactions.

These strategies may include routine risk-based reviews of high risk transactions for identity fraud that should have prescriptive assurance levels determined at an ecosystem level. These would include transactions where a user makes changes to their identity documentation used as the basis for providing verification in the ecosystem such as a passport or birth certificate.

Scope of the Legislation

In order for the Digital Identity system to move beyond the current pilot phase for wider use by the public and private sector (i.e. Financial Services Institutions, Department of Home Affairs, Services Australia, Department of Education Skills and Employment, Australian Electoral Commission, Australian Bureau of Statistics, State and Local Government) consideration must be given to the future state of the Digital Identity system to support broadening the implementation of the TDIF and roadmap of use cases that are not currently catered for by Identity Providers.

This includes but is not limited to international users, considering how verification of identities would be completed given that current documentation and liveness checks rely on the Document Verification Service (DVS) and Face Verification Service (FVS) which only hold records of Australian citizens or those who have a visa through the Department of Home Affairs.

Consideration should also be given to how the Government will build public trust towards the system, by educating and developing the public's awareness of the security measures built into the system, the importance of using supported devices for their Digital Identity collateral to avoid security risk, and having a good understanding of what information is being collected and for what purpose.

Australia is not the only country grappling with developing their Digital Identity system. It is a challenge that is being examined and tackled globally in a myriad of ways using different approaches and models with varying degrees of success. Some global examples include:

- **United Kingdom (UK.GOV Verify):** Due to the formative influence that the United Kingdom had on Australia's legal and political culture, there are important lessons from the limitations of the UK.GOV Verify model which should be considered in the Australian context. UK.GOV Verify can be described as a 'Government Directed' model in which the Government builds rules and guidelines for the ecosystem and relies on private sector response to all requirements. This model however continues to suffer from its limited focus on key digital service targets and the lack of a core Government provided public identity option (also referred to as a Government Identity Backstop). A 2019 National Audit Office investigation into the program found that in part because of this Government Directed model, the program was not on track to meet user targets, had onboarded less than half of the desired Government services and the economic benefits of the system have been found to be 75% lower than its original estimate.[6]
- **Singapore (SingPass):** The Singaporean Government has pursued a Digital Identity model that relies on a Government backstop of identity and a directed ecosystem. The core identity is managed by the Government (via the Government Technology Agency) with a view to attracting investment from the private sector to build a sustainable ecosystem. SingPass enables private sector organisations such as banks and small businesses to leverage elements of the identity solution for facial verification or account registration, avoiding the cost of developing these capabilities in-house. While the legal and political culture of Singapore is less closely aligned to the Australian context, the success of the Government backstop model at attracting private sector buy-in and sustained ecosystem usage poses important lessons for the Australian Digital Identity ecosystem.
- **Canada (Pan-Canadian Trust Framework):** The Canadian Government has to date pursued Digital Identity primarily at the Provincial level. Individual provinces such as Alberta and British Columbia have developed their own Digital Identity solutions, that have been largely guided by Provincial level strategic plans and initiatives such as the Government of Alberta IMT 5-Year Strategic Plan.[7] These solutions have adopted a 'Government Only' model in which the Provincial Government establishes the identity, the network and is the prime controlling entity for all exchange. The Canadian Government has recently developed a National level approach referred to as the Pan-Canadian Trust Framework (PCTF) that seeks to standardise and develop trust, interoperability and future private sector integration across the disparate provincial level identities ecosystems. While Australia's Digital Identity model has focused primarily on a Federal solution, the PCTF represents a valuable insight into managing disparate state based identity solutions. If Australia's states and territories opt to develop their own identity offerings to citizens, Australia may need to heed the PCTF's lessons on managing dependencies and differences between jurisdictions while balancing a unified ecosystem with broadly accepted standards.
- **Europe (eIDAS):** At the macro international level the European Electronic Identification, Authentication and Trust Services (eIDAS) regulation highlights a model for potential cross-State Digital Identity integration. It provides overarching high-level guidance that can be implemented as each nation deems appropriate with the key principle of interoperability as an underlying support mechanism. For example in 2017, Germany, Austria and the Netherlands conducted a pilot in which they connected their identity and authentication infrastructure in

[6] Great Britain. National Audit Office (2019). *Cabinet Office Investigation into Verify*. London (HC 1926 SESSION 2017–2019) https://www.nao.org.uk/wp-content/uploads/2019/03/Investigation-into-verify.pdf

[7] Government of Alberta Information Management & Technology 5 Year Strategic Plan (2016-2021) https://open.alberta.ca/dataset/01fa54bb-2827-4e87-a3d1-b3cecb59d5f8/resource/d4f8d9b7-07e1-4df6-9d48-691b5e9b54a1/download/goaimtspfinal.pdf

accordance with eIDAS, enabling Austrian and German eIDs to access Dutch online government services.[8] This broad and flexible implementation model is reflective of the complex political and jurisdictional structure of the EU, and thus may have limited immediate applications to the Australian context. However, as Australia considers potential future use cases of its Digital Identity system such as providing non-Australian citizens working in Australia with a means to pay taxes online, it is important to consider potential international interoperability while developing the Digital Identity legislation.

Our experience globally has demonstrated that a broad definition of Digital Identity is required for future proofing Digital Identity legislation. For Australia to ensure our solution remains interoperable into the future, lessons from our global peers should be considered as we develop a definition of Digital Identity that looks beyond the TDIF model to avoid restricting future use cases and scope. This should be consistent with definitions of personal, sensitive or protected information in other Commonwealth Acts while supporting the wider scope of digital use as a credential. In particular, the definition of Digital Identity and the scope of the legislation should be sensitive to anti-discrimination considerations encompassing citizens' right to privacy and ability to engage with services that align with their expectations and needs.

The Canadian model for defining Digital Identity provides a valuable case study due to its similarities to the Australian context. The Canadian model, whilst not being overly prescriptive, provides examples of the various formats that can be used as well as its purpose for use.

The PCTF defines Digital Identity as "*a type of Digital Representation that uniquely identifies a [subject] within a context, and that a user presents/uses exclusively to represent the [subject] when they access online services*".[9] Canada's framework clearly distinguishes between digital representations such as passport chip data or digital wallets, and physical representations of identity such as driver's licenses or birth certificates. Further defined terms are also used to distinguish between identity attributes, credentials and authenticators (specific identity attributes which can be used to verify user identity, based on something the user is, has or knows).

Another model for consideration is Europe's eIDAS framework, which is also useful in defining at a very high level what Digital Identity is. For example the definition of *"'electronic identification' is given to mean the process of: using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person."*[10]

It should be noted however, that the environment in which this definition and approach applies is very different in its nature to the Australian context although should be considered for a broader perspective.

It will be extremely important to define the scope early on in the development process for the proposed legislation. This includes defining key terms used such as Digital Identity and Digital Identity information, as terms can have very different meanings depending on the scope, model and context in which they are used in Australia.

There are currently a number of models for Digital Identity management that could still be interoperable under the TDIF standards whilst the proposed legislation is being developed. A well defined scope of what will or won't be covered is key. Part of this would be defining the scope of the Digital Identity components and how they will be addressed. For example, clearly defining what will be covered at a policy and framework level, who will be impacted by this, as well as clearly defining what forms of Digital Identity use will not be included in the legislation.

[8] European Commission: Access to the European publics with nation eID is becoming possible (2017) https://ec.europa.eu/digital-single-market/en/news/access-european-public-services-national-eid-becoming-possible

[9] Pan-Canadian Trust Framework, https://diacc.ca/trust-framework/

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN :page 83, article 3

The liability framework

As the legislation consultation paper doesn't specifically define the Digital Identity liability framework, we recommend that the DTA undertakes further consultation once some broad concepts that will underpin the liability framework are developed. We however, make the following observations for consideration.

In order to manage risk, security and fraud elements, as well as governance across the overall Digital Identity model, the Oversight Authority will be a critical component of the ecosystem, with its functional and operational capability tied to that of the Digital Identity system, particularly the central exchange.

This may not mean a central repository but a central point where information can be aggregated when required, as in the case of biometrics. While preserving the privacy of end users, the current double blind model creates unique oversight challenges due to the difficulty of obtaining end-to-end visibility of system transactions. While Australia plans to use the double-blind model, other comparable jurisdictions are too early in their implementation and adoption of this model to leverage lessons learned. We should however continue to monitor this as we progress with our own development.

The Oversight Authority must define its role within the broader regulatory framework. Specifically we suggest the DTA determine whether a completely bespoke liability framework is required or whether some of the same goals can be achieved by relying on existing liability frameworks, including:

- The OAIC's powers under the Privacy Act, including any additional powers that result from the Attorney-General's ongoing review;
- The contractual framework between participants in the Digital Identity system; and
- Tort claims between the parties, including fraud and negligence claims.

The shape of the liability framework will be informed by the proposed role, power and breadth of the Oversight Authority. Taking a more active role will require both additional enforcement powers and significant subject-matter expertise, which will affect the Oversight Authority's proposed financial self-sufficiency and funding model.

Considerations for liability and enforcement

A key feature of the proposed governance framework is that the Oversight Authority will have the power (either under the primary legislation or the operating rules) to suspend or terminate a participant's use of the system as a consequence of that participant's non-compliance.

Although this power is certainly necessary and consistent with other regimes, in our experience suspending or terminating one participant's use of a system can cause disruption to other participants and users. For example, suspending an attribute service provider will mean that any relying parties or end-users who depend on that attribute service provider will need to implement workarounds (such as verifying all attributes manually).

To minimise any disruption caused by this, we suggest that any 'immediate' suspension or termination rights should be confined to prescribed categories of sufficient materiality (such as a material or persistent breach of the legislative instruments, non-compliance with a direction from the Oversight Authority, or insolvency).

Where possible, any suspension or termination rights should be exercised with appropriate notice periods to both the non-compliant participant and any other affected participants or users and, where possible, with adequate opportunities to remediate non-material breaches.

Financial sustainability of the accreditation system

The TDIF is predicated on a comprehensive accreditation process which underpins the liability framework, both at the point of the initial on-boarding of a participant and as part of an ongoing annual compliance program. A key feature of this accreditation process is that all costs must be met by the applicant / participant. Significantly the accreditation process includes third-party independent assessments of an applicant's / participant's Privacy Impact Assessments and compliance with the TDIF.

Although a robust and comprehensive compliance program is critical to maintaining user trust in the system, the costs associated with participating in the system are likely to be a barrier to entry for many smaller private sector organisations.

As noted in the consultation paper, many potential participants are smaller companies in the technology sector and the cost threshold may be too high for this sector.

For many years, this was a key feature of Australia and the UK's payments system whereby the high costs associated with accessing the payments infrastructure required to securely process payments coupled with expensive ongoing compliance obligations led to an uncompetitive payments regime made up of big banks. The high cost of meeting accreditation requirements has similarly inhibited adoption of the Consumer Data Right in Australia.

The UK in particular has taken steps to remedy high costs of accreditation by adapting the regime to address these cost impediments and foster participation by smaller FinTech companies.

When seeking to balance the desire to encourage participation with the desire to maintain the integrity of the system, a possible approach is to adopt a 'tiered' approach to compliance. For example, the Payment Card Industry Data Security Standard separates participants into tiers by reference to (amongst other things) the number of transactions that each participant processes in a year. This tier then informs whether the participant must obtain a third-party independent assessment and undertake external penetration testing or whether a self-assessment and attestation of compliance in each year is sufficient. We suggest that this be considered for the proposed Digital Identity system.

3. Safeguards

The importance of privacy

As noted previously, enshrining privacy protections in primary legislation underscores the fundamental importance of these protections. This should be balanced with flexibility as not to unintentionally restrict their scope by defining the requirements too specifically.

The incorporation of principle-based privacy safeguards in the Digital Identity legislation will be an important mechanism for protecting the privacy rights of Australians to exercise control over their personal information and clearly understand what information will be collected, used and disclosed.

Privacy is not only an end in itself, but key to the realisation of a number of other related rights such as freedom of expression and freedom from discrimination. The recent history of high profile data breaches, data misuses and increased legislative and regulatory attention demonstrates that preserving privacy in technology is critical to establishing trust in digital systems and driving engagement.

Measures that protect privacy through governance and oversight processes, such as existing TDIF requirements to complete Privacy Impact Assessments, designate a Privacy Officer or publish a dedicated privacy policy,[11] may be most appropriately embedded in legislation. Governance and oversight requirements are independent of specific solutions implemented in the Digital Identity system and are unlikely to be impacted by innovation and technology change.

Care should also be taken to ensure that legislated privacy safeguards are aligned to requirements under the *Privacy Act*, for which significant reform is anticipated within the next 12-24 months. Consistency with the *Privacy Act* will ensure that compliance burdens on Identity Providers and relying parties are streamlined and opportunities for system participation are maximised.

Conversely, protective security and privacy engineering best practices, such as existing TDIF requirements found in Section 4.2 Information Security should be flexible enough to be updated in response to changing threats and technology innovation. Requirements such as these may be more appropriately maintained in technical standards documents developed by the Oversight Authority, in consultation with system participants.

Choice

Voluntary participation will be critical to build public trust, secure community buy-in of the system, and prevent exclusion of individuals with barriers to accessing digital services. For example, due to restricted access to devices or lower levels of digital literacy.

From an accessibility perspective especially in relation to access to Government services, not everyone will want or be able to participate in the proposed Digital Identity system for a variety of reasons. Offline access to services should remain available for those requiring or choosing this option. We would suggest consultation with communities that may be disproportionately impacted by the introduction of the Digital Identity system, to ensure their specific needs are considered as the system develops.

Restrictions on data profiling

We suggest that restrictions on the use of behavioural information within the legislation should continue to be guided by the core functions performed by system participants rather than by information type. This has been the approach of the TDIF, which restricts the collection, use and

[11] TDIF Release 4: Functional Requirements, pp. 10-20.

disclosure of information about an individual's behaviour to very specific identity verification, fraud management and system refinement functions.

This focus on restricting the sharing of behavioural information based on essential system functions is particularly important given the rapidly changing availability of attributes of the user end. For example, we saw privacy changes within the Android 10 Operating System in February 2020 make device identifiers such as the Device ID attribute significantly more challenging to access by mobile applications. If a change like this were to occur during the operation of an Australian Government managed identity fraud system, the ability for Identity Providers, relying parties or the Oversight Authority to meet their fraud management obligations could be significantly impaired.

Further, if a stringent list of approved and restricted behavioural information types enforced by legislation existed, system participants may be unable to substitute this missing core attribute in their identity fraud detection engines or systems, potentially exposing citizens to fraud.

In order to protect citizens and keep pace with an ever evolving fraud landscape, there needs to be a degree of flexibility in the behavioural information system participants are permitted to consume for their TDIF approved core functions.

The consultation paper appears to be subscribing to a similar approach as it proposes limits on the use of a user's behavioural information collected on the system, especially to prohibit:

- activities such as direct marketing
- the sale of information for direct marketing, and
- generalised compliance activities by the Government

To avoid sharing behavioural information across the system, the legislation should consider mandating a risk scoring system based on a standardised approach across the network. This may resemble the process currently employed by DVS and FVS where information indicating the risk associated with an individual's authentication is distributed to system participants via standardised alerts/messages, rather than information associated with the document or the biometric itself.

This kind of risk score based on a standardised approach could be shared across the network, and managed by the Oversight Authority.

A further consideration is the sharing of any confirmed identity fraud attempts detected by the system through the use of data profiling with industry intelligence exchange companies, such as the Australian Financial Crimes Exchange (AFCX) in an effort to enhance identity takeover (IDTO) preventative measures across the Financial Services sector in turn improving the protection of Australian citizens.

The reference to the Digital Identity Participant Register in the consultation paper is a positive element for registered users to be able to access a list of who the registered participants are and what attributes they are authorised to receive. That said, we would caution this information being publicly available to all and suggest that it is perhaps limited to registered users and participants to avoid the potential for scams and misuse of information.

We further urge the need for public education and awareness around how participants would be enabled to access their authorised attributes and suggest that this is restricted to registered users and participants.

A further suggestion would be for the Oversight Authority to conduct periodic assurance across authorised requests for access to restricted attributes to ensure justifications and approvals are appropriate. Users who have previously granted release of restricted attributes should have an appeal and retraction process available should they decide to reverse their consent.

Biometrics

As the consultation paper highlights, Biometric Information is personally identifiable and cannot easily be changed. Unlike the other common factors of authentication such as 'something you know' or 'something you have', the permanence of biometrics, 'something you are', produces a unique insecurity.

Unlike passwords or tokens, in the event that an individual's Biometric Information is compromised, biological attributes cannot be revoked or reset.

Expanding the footprint of biometrics in the system beyond the initial identity proofing use case may introduce new, potentially unacceptable risk if not appropriately secured. In particular, expanding biometrics to a credential provider managed authentication use case may result in a distribution of Biometric Information to multiple types of actors in the system that are currently held to different legislative standards. This would represent a significant departure from the current position of the TDIF which mandates that no entity other than the Department of Home Affairs can hold the facial Biometric Information used for identity proofing.

It is our view that if the system is to move towards a model in which credential service providers are permitted to encrypt and store their Biometric Information for authentication purposes the DTA should consider:

- Ensuring that the Legislation develops safeguards, such as tightly defined limitations in the use of Biometric Information for these new, uncharted authentication use cases,
- Developing mandatory technical requirements within the TDIF that sit parallel to the Legislation, instructing relevant Accredited credential providers on how to securely encrypt and store Biometric Information,
- Enshrining Persistent Attack Detection (PAD) and Liveness requirements in both the Legislation and TDIF.

As Australia's Digital Identity landscape matures and Biometric Information is potentially held by multiple trusted entities within the system, it is possible that a requirement may arise to link some of this Biometric Information. PwC's experience working with the *Common Identity Repository* in Europe, for instance, highlights that as disparate biometric databases develop, so too does the need for a shared biometric matching service to detect multiple/fraudulent identities or to execute high risk transactions. For example, if an Australian Digital Identity user is seeking to change a detail of a Category A Identity document (e.g. Gender assigned at birth on a Birth Certificate) a future system may require step-up authentication that links multiple pieces of Biometric Information that may be distributed across Federal, State/Territory, and Credential services provider databases.

The DTA should consider if any of its proposed safeguards on the use of Biometric Information in the legislation would restrict a future system from developing a service that is capable of verifying Biometric Information from multiple sources without developing a single, high risk central repository.

Consent, Opt-Out & Authorised Representatives

We are supportive of a strong user consent concept being embedded in the legislation. For consent to be meaningful and valid, users must be adequately informed of the system actions to which they are agreeing. Regulators in the E.U. have developed guidance on the standard of consent, for the purposes of regulating the General Data Protection Regulation (GDPR), which may be applied in these circumstances. The ICO in the U.K., for example, advises that valid consent must involve 'genuine choice', be specific, concise and readily understood.[12]

In line with this, we are supportive that a mechanism requiring individual's consent before a user transacts to a relying party is a key control to preventing identity take over risk and should be specifically provided in the legislation. A consent verification action at this stage is a useful form of friction that provides a second factor verification step, while also presenting an opportunity to explain what data is being verified, for what purpose, and to record user consent.

Furthermore, we are supportive of an opt-out mechanism being available should there be a change in circumstances, with users clearly advised of the information retained by the system. To protect the autonomy of Digital Identity system participants, it is

[12] Information Commissioner's Office, *Guide to the General Data Protection Regulation* 'What is valid consent?', available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/

important that users are able to withdraw their consent to participate or 'opt-out'. This will require Identity Providers to apply clear data management controls to ensure the personal information of 'opted-out' users cannot continue to be used once a user withdraws, while also retaining sufficient audit records of prior transactions.

We would suggest that unlike other data exchange frameworks, such as the Consumer Data Right or the My Health Record system, which permit deletion of personal information on request of the consumer, it would not be appropriate that identity verification transaction data is destroyed as this may threaten the integrity of the system and the ability of the Oversight Authority to investigate incidents of fraud. Users electing to 'opt-out' or withdraw consent should receive clear information about what personal information will continue to be retained by the Digital Identity system operator. Consideration should also be given to the ability for third parties to act on behalf of users.

Currently the system only supports situations where a user needs to act on behalf of a business. There are many other occasions where a user may need someone to act on their behalf when accessing government services, including payments being moved directly from a benefits payment or where a user does not have the ability to use services or lacks legal capacity.

We suggest there should also be capability to remove or restore the identity if it is proven to have been established or amended as a result of identity takeover or synthetic identities.

Age

The minimum age for participation in the Digital Identity system should be aligned to the ages at which individuals are able to be assigned and control Government identifiers (e.g. in NSW a person is eligible to apply for a proof of identity card or apply for learners drivers license at 16 years of age). This would also be consistent with the minimum age at which an individual can legally provide consent. This varies on the act consented to, but 16 (age of consent laws) and 18 (entering into contracts if contract not to their benefit).

However, we do note that this approach (participation from 16 years) would be inconsistent with other Government services and guidance, including:

- The OAIC recommendation that any person over 15 can be assumed to have the capacity to provide consent (unless there are circumstances indicating that the individual lacks capacity)
- The minimum age for having a separate Medicare card, 15 years. In this case we recommend harmonising with this if a mismatch would reduce access to health services; and
- Age at which teenagers take control of their My Health Record is 14 years

It is our view that the minimum age for consent and participation in the Digital Identity system should not be confined to a question of whether an individual has legal capacity to make autonomous decisions in relation to services provided by relying parties. Consideration should also be given to the individual's capacity to understand the consequences of poorly managed privacy, secure use of devices and the risks of possible identity fraud.

Acting on behalf of another

Acting on behalf of others (e.g. where a person lacks capacity) should always be through formally defined roles, such as authorised representatives that are appropriately authorised. The legislation should include a requirement for the system to remove access by the authorised representative to the person's Digital Identity when their authority ends (e.g. because the person becomes of age, regains capacity, or a change in authorised representative). Consideration should be given to child custody and domestic violence situations in relation to disclosure of information through linked services as well as the possibility of multiple authorised representatives for a single person.

If a person is capable but merely lacks interest or motivation to engage with the system, we suggest that this be treated as an individual decision not to participate. As long as this doesn't reduce the number of services the person can access and they can still verify their identity using physical means, then the legislation should not make special provision for these cases. This should be addressed through public awareness and education campaigns.

The legislation should consider the needs of vulnerable customers. Whilst an authorised person may be permitted to represent and take actions on behalf of a vulnerable person, they may not always be acting in that individual's best interest and in turn may also be taking advantage of the Digital Identity system to fraudulently establish user profiles and digital access to relying parties.

Privacy Impact Assessments

Privacy Impact Assessments (PIA) are a valuable process that enables organisations to document personal information data flows and understand when that data may be shared within their own organisation and across external entities. They provide an opportunity for privacy specialists to review initiatives and identify any associated privacy risks, which may then be appropriately mitigated or treated.

PIAs are widely considered better practice in many large organisations, but not currently mandated by Commonwealth Privacy Act 1988. We would suggest the operating rules are the preferred option for the PIA requirement as primary legislation would be too inflexible. This would also align with how the requirement for PIAs of high risk projects by federal Government agencies is captured in the legislative instrument[13] rather than the primary legislation.

Ideally, Privacy Impact Assessments should be conducted in conjunction with Privacy-by-Design processes to ensure that solutions minimise data collection to only that which is necessary, default configuration is always privacy protective, and privacy best practices are embedded in requirements and considered as core solution functionality. For Government services, these protections should be ingrained as part of the organisations mandate and provisioning of services. Regular stakeholder consultation at both a solution and system level should be embedded as part of each phase of the development of the Digital Identity system system with members of the disability community.

[13] Privacy (Australia Government Agencies - Governance) APP Code 2017

Accessibility and anti-discrimination

Support for accessibility should involve consultation with the disability community to ensure voices are heard and that solutions are codesigned rather than specific coverage in legislation, though access to Government services through a variety of forms e.g. offline via phone and in person should and is enforced at an agency level to ensure all users have access to services.

This legislation and the Digital Identity system should take into account that not everyone will be able to or want to participate in the system and will still require suitable offline options for proving their identity and interacting with relying parties.

Accessible design and community consultation should also take into account the needs of culturally and linguistically diverse (CALD) communities, to ensure that system messaging and public information campaigns are effectively communicated and are not exclusive.

Disclosure of personal information

Current accreditation requirements under TDIF require accredited participants to 'opt-in' to Privacy Act coverage, if they are not already within the scope of the legislation. This means that Digital Identity system participants will be restricted in the range of

scenarios in which personal information can be disclosed by APP 6, including circumstances such as:

- In accordance with court or tribunal orders, or
- Where necessary for the activities of a law or regulatory enforcement body[14]
- Where there may be a threat to life, health or safety, to locate a missing person
- For establishing legal claims
- For diplomatic or consular activities
- For the purposes of conducting war, peacekeeping or humanitarian operations[15]
- 'Permitted health situations' further provides a range of scenarios in the context of health care and public health policy that can allow personal information to be disclosed for the purposes of establishing familial medical history, conducting public health research, and providing genetic counselling to relatives.[16]

Provisions detailing exceptional circumstances in which information may be disclosed should, therefore, not need to be replicated in legislation governing the Digital Identity system. The goal of any additional disclosure obligations under this regime should be customised to the unique needs of the Digital Identity system, and the particular sensitivity of the information it will handle.

It should be noted that disclosures of personal information without consent (under APP 6) that are 'reasonably necessary for one or more enforcement related activities' may not align to public expectations.[17] 'Enforcement related activities' is worded broadly and does not necessarily require that enforcement agencies produce a warrant or court order for disclosure to be lawfully made. The definition of 'enforcement bodies' is not confined to Federal and State law enforcement agencies, but also includes the Department of Immigration, APRA, ASIC and various independent anti-corruption bodies. Conceivably, APP 6 could permit disclosure of Digital Identity biometric data by Identity Providers to enforcement bodies, without the requirement that the individual concerned be under any particularised suspicion.

Focus should instead be on ensuring that information about user activity can be appropriately used and disclosed for the purposes of investigating fraudulent activity in the Digital Identity system, and which could be covered by similar access provisions as currently enshrined in the *My Health Records Act 2012*.

The My Health Record (MHR) system currently permits disclosure of MHR data only for a limited range of purposes, such as management of the MHR system; to prevent serious threats to life, health or safety; with the record holder's consent; under court or tribunal order; or to investigate unlawful activity in relation to the MHR system.[18]

Notably, the MHR legislation has provided a list of prohibited purposes for which MHR system data should never be used. The Digital Identity system should also consider similar prohibitive provisions to give Australians confidence that data collected for the purposes of accessing services and verifying identity will not be used for purposes with which there is considerable community unease. The OAIC Australian Community Attitudes to Privacy Survey provided clear data that Australians are generally more comfortable with government uses of personal information than they are with commercial uses.[19] Likewise, the ACCC's Digital Platforms Inquiry also gathered data on the increasing levels of discomfort Australian consumers have with data practices that use personal information for purposes other than those related to the provision of a service, such as monitoring online behaviours, developing profiles for targeted advertising, and disclosing data to third parties without the individual's knowledge.[20]

[14] Privacy Act 1988 (Cth), Schedule 1, Australian Privacy Principles, APP 6.2.
[15] Privacy Act 1988 (Cth), section 16A (1).
[16] Privacy Act 1988 (Cth), section 16B.
[17] Privacy Act 1988 (Cth), Schedule 1, Australian Privacy Principles 6.2 (e).
[18] My Health Records Act 2012 (Cth), sections 63 - 70.
[19] The OAIC Australian Community Attitudes to Privacy Survey, available at https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/
[20] Consumer Views & Behaviours on Digital Platforms, Final Report 2018, prepared for the Australian Competition and Consumer Commission, available at https://www.accc.gov.au/system/files/ACCC%20consumer%20survey%20-%20Consumer%20views%20and%20behaviours%20on%20digital%20platforms%2C%20Roy%20Morgan%20Research.pdf

To build public trust in the Digital Identity system, prohibited uses of personal information should include commercial profiling, targeting and behavioural analysis (other than as required for anti-fraud measures), reflecting the findings of this research into attitudes on data practices.

We think it will be important for the legislation to be clearly scoped and ensure that distinction is made between personal information already held by identity service providers and attribute service providers, and used for the purposes of verifying identity (e.g. passport, birth certificate or drivers' license data), versus the data collected specifically as a result of user activity in the Digital Identity exchange (e.g. transaction audit logs).

Ensuring the public understands there are clear limits to the use and disclosure of Digital Identity exchange data for secondary purposes will assist in allaying fears about the creation of a national surveillance database. Successful adoption will require that the community has confidence it understands how personal information is being used and to which other Government agencies it will be disclosed.

4. Governance

Functions and activities of the Oversight Authority

As outlined above, the role of the Oversight Authority is a key component to ensuring the risk, security, fraud management and overall governance of the Digital Identity system is effectively monitored for the best interests of the Australian public.

The functionality, responsibilities and governance role the Oversight Authority plays needs to support adaptability and agility as the Digital Identity system evolves and matures - this will enable it to perform its operational and oversight roles effectively.

The role of the Oversight Authority should cover the management of key activities needing a level of oversight across the entire system, for example governance, trust, risk, onboarding new participants, fraud monitoring requiring the removal of the double blind. This functionality is linked to the exchange and requires a strong mature capability.

The skill set for those involved would be diverse with required capabilities ranging from system governance, cybersecurity, preventative fraud monitoring for a range of events, technical support and governance across the system, fraud investigation and 24/7 monitoring capability.

The Oversight Authority will, in addition to its governance role, do a combination of fraud and security monitoring, having the capability to adapt and react to a daily changing threat landscape. Preventative monitoring of the system overall will be key, alongside the need for independence and transparency. This functional capability is currently planned to be uplifted at the same as the government has increased investment in cyber as part of the 2020 cyber strategy which includes the development of 3 cyber hubs to support the whole of Government cyber resilience.

Trust mark

The establishment of a Trust Mark to signify an entity's accreditation provides users with a level of confidence and trust that entities have passed the stringent requirements governed by the Oversight Authority for the protection of users. Given the fraught history the Australian public has with trusting the secure storage and use of personal data in a Government context which has been further amplified by the recent spoofing attacks that have been rampant during COVID-19, a Trust Mark will be an important element in upholding public trust.

A global example of where a Trust Mark has been developed successfully is the approach taken for eIDAS. We must note that the principles of this framework put privacy and data security controls at the forefront of its design and are therefore different to the approach previously taken in Australia.

Previous Australian Government experience demonstrates the expectation of the public for privacy and data security to be front and centre in the design and management of trusted identity credentials. Failure to do so has the potential to lead to reputational risk and public scrutiny.

This concern has been raised with previous PKI solutions such as AUSkey. The strong level of trust in the credential, if used in an unmonitored manner and beyond the original intended use and without the support of the provider will increase the opportunity for fraud and security breaches.

Any public trust in the use of Digital Identity credentials or the system itself will be eroded through unmonitored fraudulent activity or events occurring outside of Digital Identity system and the TDIF. The scope then of where and how a trust mark should be used needs to be considered. Whether this needs to be enabled through legislation or as part of the policy framework should also be considered

5. Interactions with other policies, programs and laws

Consistency across Australia

As part of its accreditation process, any participant must be subject to the Privacy Act (or equivalent provisions), reinforcing that compliance with the Privacy Act will underpin participation in the Digital Identity system.

It is intended that this requirement will be transposed into the legislation or the legislative instruments. Although this is likely to be non-contentious for the majority of participants (that are Government agencies or large private sector entities that meet or exceed the $3 million annual revenue threshold),

where a participant is a smaller company (such as a start-up technology company) that entity will need to 'opt-in' to the Privacy Act in accordance with Section 6EA in order to become a registered participant.

In our experience, entities that chose to 'opt-in' under this provision are often not-for-profit entities and charities that do so as part of a broader ethos around good privacy practice and to build confidence and trust. This means that the processes around 'opting-in' are relatively straightforward and managed solely through the updating of a publicly available 'opt-in' register.

With this in mind, any entity that 'opts-in' to the Privacy Act is free to 'opt-out' at any time. This means that if ongoing compliance with the Privacy Act was a prerequisite for registration as a participant, confirmation of 'opting-in' may not be sufficient to satisfy the objectives of the Digital Identity system. To manage this, the Oversight Authority may need to have more oversight over its participants and their ongoing compliance with the Privacy Act. For example, the Oversight Authority could consider implementing a data link with the OAIC's 'opt-in' register so that any 'opt-out' automatically results in a suspension or termination of that participant from the Digital Identity system.

In addition to compliance with the Privacy Act, relying parties providing services may also be required under specific legislation to manage, store and share data in a specific way. It is recommended that a review of the broader legislative environment for both accredited entities and service providers who will interact in this system be undertaken to ensure consistency in application across the ecosystem. For example: systems such as Medicare, Centrelink or the My Health Record, the legislation is quite specific about not being able to collect data if it doesn't pertain to the application for the benefit/service. This should be congruent with principles proposed in the Digital Identity legislation

Consistency of privacy protections

The TDIF currently imposes a data breach reporting obligation on each participant[21]. This obligation is defined by reference to the notifiable data breach regime under the Privacy Act but further requires the participant to notify the Oversight Authority, the DTA and any 'affected individual.'

This is slightly inconsistent with the *Privacy Act* where s26WL(2) requires entities to notify "individuals to whom the relevant information relates." If the notification obligations under the legislation are likely to be more extensive and will extend to any other participant in the system, the Oversight Authority should consider whether this should be reflected in the permitted time frame for notifications. The TDIF currently provides no guidance in relation to this.

[21] Functional Requirement 3.4.

6. Conclusion

The development of the Digital Identity legislation is required to keep pace with technology and the needs of businesses. An enhanced legislative framework for the Digital Identity system will be a positive step forward from the TDIF model. We acknowledge the work that the Government has done, with the TDIF and programs such as Digital Identity system, to lay the foundations for a comprehensive, fit for purpose, Digital Identity system in Australia.

While in agreement that an enhanced legislative framework is the next step, this is a challenging policy area that will require a collaborative effort between industry, government and other Digital Identity players to achieve success. Key to this success, will be consideration of the following key points:

- Australia is not unique in addressing this challenge - there is much to learn from the global experience of other countries and thought leadership available. We have sought to highlight this in our answers above.
- It will be critical to strike the right balance between a legislative framework that provides strong governance and one that is flexible enough to adapt to rapid change that is omnipresent in this space.
- Balance will also need to be found between making data accessible enough that the system works and keeping that data secure and maintaining the public's trust.
- Buy-in from the private sector will be critical to driving adoption. From our own experience, we know that a number of private sector organisations have programs in-flight to develop their own identity credentials and are looking for clear guidance on how their identity credential programs will sit alongside a Government developed identity system. Interoperability between private and public sector organisations will drive economic benefits by making it easier to access services and by efficiently leveraging identity verification from trusted sources of truth.

7. Index

Consultation paper questions

12a	Are there any other safeguards on Biometric information that should be included in the Legislation?	3 - Safeguards, pg 13-14
12b	Are there any that have been proposed above that should be modified or excluded, and if so, why?	3 - Safeguards, pg 14
13a	Do you agree with the proposed approach for Biometric Information?	3 - Safeguards, pg 14
13b	Will the limitations on Biometric Information overly constrain innovation or rule out legitimate future use cases?	3 - Safeguards, pg 14
14a	Should the Legislation specifically provide a mechanism requiring an individual's consent before the User transacts with a relying party?	3 - Safeguards, pg 14
14b	Should the Legislation specifically provide an opt-out mechanism enabling individuals to opt out of the system after they have created a Digital Identity?	3 - Safeguards, pg 14
15	Should there be a minimum age set for a person to be permitted to create their own Digital Identity? If so, what should it be?	3 - Safeguards, pg 15
16	How should the Legislation cover situations where a person lacks capacity, is not capable, is too young or lacks interest or motivation to engage personally with the system?	3 - Safeguards, pg 15
17	Should the requirement for a PIA remain in TDIF accreditation requirements or should it be required in the Legislation or Operating Rules?	3 - Safeguards, pg 17
18	In addition to the right to privacy and anti-discrimination in relation to accessibility and disability, how should the Legislation safeguard and ensure the enjoyment of Australians' human rights?	3 - Safeguards, pg 17
19	Is the proposed approach to accessibility and usability practical and appropriate? Should any other considerations be taken into account?	3 - Safeguards, pg 17
21	Should the Legislation include provisions to enable the disclosure of information in specified circumstances? If so, what should those circumstances be?	3 - Safeguards, pg 17-19
22a	Are there established independent bodies that could fulfil the role of an independent Oversight Authority for Digital Identity, or is a new independent body required?	4 - Governance, pg 20
22b	What is the optimal structure of a new body?	4 - Governance, pg 20
28	What best practice models should be considered for the protection and use of the trust mark?	4 - Governance, pg 20
29	Is the proposed approach appropriately balanced to achieve the objectives of the system?	5 - Interactions with Other Policies and laws, pg 22
31	Is the proposed approach appropriate to achieve a high degree of consistency of privacy protections?	5 - Interactions with Other Policies and laws, pg 22

8. Contacts

Corinne Best
Trust & Risk Business Leader
corinne.best@pwc.com

Mary Attard
National Digital Identity Lead
mary.attard@pwc.com

Mike Cerny
Partner, Cyber Security & Digital Trust
michael.cerny@pwc.com

Nicola Nicol
Partner, Cyber Security & Digital Trust
nicola.nicol@pwc.com

Jon Benson
Partner, Cyber Security & Digital Trust
jon.benson@pwc.com

Adrian Chotar
Partner, Cyber Security & Digital Trust
adrian.chotar@pwc.com