www.iispartners.com

Information Integrity Solutions Pty Ltd
Building trust and innovative privacy and security solutions

24-30 Wellington St, Waterloo NSW 2017 Australia
PO Box 978, Strawberry Hills NSW 2012 Australia

Tel: +61 2 8303 2438
Fax: +61 2 9319 5754

inquiries@iispartners.com

DTA Digital Identity Legislation Submission

Information Integrity Solutions (IIS) welcomes the invitation by the Digital Transformation Agency (DTA) to receive submissions on the DTA Trusted Digital Identity Legislation. The Legislation is intended to help expand the Australian Government's Digital Identity system into a whole-of-economy Digital Identity solution by establishing robust governance, as well as strengthening data and consumer protections. The Legislation will also allow entities in other digital identity systems to apply for Trusted Digital Identity Framework (TDIF) accreditation (the TDIF accreditation scheme). The Bill is proposed to be introduced into the Parliament in late 2021.

About IIS

IIS helps public and private sector organisations embed trust, privacy, and security as core value propositions internally and in their products and services. IIS is recognised as one of the leading privacy consultants in Australia. We have extensive experience working with government agencies, companies and not-for-profit organisations. Our consulting team has strong local and international connections, deep knowledge of privacy and security, and a commitment to **moving beyond compliance to performance**:

- IIS takes not only organisational risk, but also customer and citizen risk into account
- IIS looks for solutions that meet government, business and strategic goals in ways that build trust through respectful stewardship of data.

Please see the About Us page for further information.

We hope that the DTA will consider our submission as part of the consultation process. IIS support the holistic drive by the Australian Government to help deliver a safer and more private and secure cyber world for the people of Australia, both now and well into the future.

Rationale for a Trusted Digital Identity Framework enforced by legislation

Key observations and recommendations on the legislative outline that IIS wish to make depend on a good understanding of the fundamental rationale behind it and TDIF.

At its simplest, legislation to enforce TDIF seeks to facilitate more trustworthy exchange of Verified Claims about Relevant Attributes without establishing an all seeing, all powerful Digital God.

The rationale for developing TDIF and the system that applies it is an age-old risk management challenge. Indeed, establishing a means by which two parties can reduce the risk that both face to a point where they are willing to engage each other has been addressed in many ways over the centuries.

One method is for the relying party to assess claims made by the other party. That assessment is influenced if a trusted third party can vouch for the veracity of the claim. In the digital era, a claim often verified is 'identity'. Underneath that poorly defined catch-all term is usually a varying basket of claims that are verified, for example 'name', birthdate, residential address but also evidence of long-term presence in society through presentation of years of utility invoices, presence on the Electoral Roll etc.

However, verification of inappropriate claims or their inappropriate sharing and use creates very well documented and significant privacy risk to individuals and security risk to both parties.

Hence the simplest way of thinking about the optimal approach to this kind of solution to the risk management challenge is to see it as an exchange of:

Verified Claims about Relevant Attributes

This is illustrated by very a simple example: to enter licensed premises, the claim that is relevant is whether the individual is over the legal drinking age. Any claim about birthdate or name is not relevant. If that claim is vouched for by a trusted third party, then the licensee is more likely to accept the claim as correct.

The processes usually implemented in the digital era create new risks if parameters about the claim making and verification are also recorded, such as time and location of presentation, who is the relying party etc and hence lifestyle patterns adduced.

The risk to individuals increases if there is only one verifying party. If the verifying party chooses not to create a digital 'identity' or chooses not to verify claims made about that 'identity' or cancels it or simply makes a mistake, the individual potentially has nowhere to turn for relief. The verifying party is also often able to monitor all verifications of the claims made during individual's use of that 'identity'.

If that ‘identity’ must also be used for leading almost all aspects of life, then such an arrangement is creating:

The Digital God problem

A Digital God model might be appropriate for certain relationships, for example the employer/employee arrangement for employment purposes. However, Australians have repeatedly rejected such asymmetric power constructs for leading life in general, especially if the Digital God is a government. The failed Australia Card and Access Card initiatives are the two most notable examples in recent decades.

The Trusted Digital Identity Framework that has been developed over the years by the Digital Transformation Authority and others seeks to verify claims about relevant attributes while avoiding the emergence of a Digital God.

TDIF also seeks to relieve both the individual and relying parties from the burden of having to obtain, manage and present the different ‘identities’ that different relying parties might seek to implement. It sets out to do this through a series of interoperability requirements.

TDIF seeks to achieve all these objectives by separating the relying party from the verifying party. Under TDIF, neither of those two parties is able to know anything about the other. They are ‘blinded’ to each other through an intermediary.

TDIF seeks to make the system more trustworthy and interoperable through the technological construct behind it, the compliance and assurances it obtains from participating parties and the promises the intermediary also makes that it too will do the right thing in terms of security and privacy.

The intermediary and the system also need to ‘keep their word’ over the very long term – years. ‘Function Creep’ that might undermine the original construct and hence its trustworthiness is potentially a critical weakness.

Over the years, it has become clearer that the necessary level of trustworthiness in the intermediary, the system as a whole and TDIF itself can only possibly be achieved through legislative backing, not simply by contracts between all parties.

On this basis, IIS submits the following observations and recommendations on the proposals in the Position Paper.

IIS Key Observations and Recommendations on legislative Position Paper

IIS supports the fundamental construct of the TDIF as a way to deliver more trustworthy exchange of Verified Claims about Relevant Attributes without establishing an all seeing, all powerful Digital God. IIS considers that legislative support and enforcement of TDIF is vital if the system is to be sufficiently trustworthy.

Legislation also helps to ensure that the original intent of the system endures over time and can only evolve by agreement of the people's elected representatives rather than through administrative whim.

In designing the legislation, it is vital to recognise that digital identities obtained and verified through TDIF are likely to dominate every aspect the lives of individuals as digital continues to increase its dominance of how lives, business and government are conducted. Indeed, the policy intent is that TDIF facilitates this evolution.

As a consequence, both TDIF and the legislation behind it must be fit for purpose over the long term even when any failure or error could bring an individual's life to a grinding halt. If one of the consequences is lifelong identity takeover, the impact could last the rest of their lives and offer serious harm.

Bearing these considerations in mind, the discussion paper outlines a good legislative infrastructure. IIS agrees with the majority of the Position Paper and where we do not comment it implies general agreement.

Overall, more emphasis needs to be placed on the system being respectful of Users as individual people not just economic units and be symmetric in its treatment of the parties.

Our main concerns are:

- Ensuring that Users / advocates will have continuing and genuine influence as the system evolves.
- Effective governance, compliance, enforcement, and remediation/redress for the individual User.
- Protection from (or genuine oversight of) surveillance by law enforcement and national security agencies (including the interaction between this legislation, the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020).
- Ensuring that alternatives to using the TDIF system continue to be available for years to come, if not forever. If alternatives are not practical, too cumbersome, simply not provided or coercion forces the use of digital identities created by the TDIF system, then any 'consent' is rendered meaningless and arguably, invalid in law. Should consent become meaningless, additional measures to improve governance, accountability, remediation, and redress will be essential.

Comments on specific elements of the Position Paper

Sections 5.3 & 5.4.7 – These sections propose that the "definition of Digital Identity information will include a non-exhaustive list of examples, with further details to be set out in the rules". They also propose that "the Bill will include a power for the Minister to specify attributes in the rules to capture all the attributes available under the TDIF rules, and to update those as they evolve over time". It appears that some protection is in the proposition that these rules are disallowable instruments by the Parliament.

However, this could lead to some form of increased surveillance if it also leads to Users not being able to lead their lives without verification of an increasing range of attributes.

IIS has particular concern about the implications of such broad conception of Digital Identity information if sensitive attributes such as racial or ethnic attributes are included. In some circumstances that attribute can be beneficial, e.g., First Nations people gaining access to additional study assistance. In other circumstances the impact can be the exact opposite as many First Nations people will testify. The answer may depend on well-funded and firm enforcement of Australia's anti-discrimination legislation and other measures recommended in the Human Rights and Technology Final Report issued by the Human Rights Commissioner earlier in 2021.

IIS recommends that the legislation should only be introduced to Parliament if it is accompanied by actual appropriation of funds to regulators including the Human Rights Commission and the Office of the Australian Information Commissioner (OAIC) that enable them to enforce and remediate such harms. If that is not possible, IIS recommends that the legislation should be accompanied a joint public statement to Parliament by the Minister responsible for the legislation and the Minister for Finance that commits the Government to provide specified additional funding.

Section 5.4.10 – "It is proposed the TDIF rules to be made by the Minister will include definitions of identity proofing, re-proofing, authentication, verification and credential" and "The definition of re-proofing will include an exhaustive list of the permitted purposes for re-proofing".

In a worst-case scenario, this power could be used to create a class of 'non-people' for example undocumented migrants.

IIS recommends that the legislation confirms that exercise of this power is not only a disallowable instrument (as appears to be the case if it is a TDIF rule) but that individual adverse decisions in its application also be appealable to the courts.

Section 5.4.13 – "The Legislation will not prohibit Participants from connecting to and participating in other digital identity systems". The implications of this for any Users whose identity is compromised in such a complex system need to be addressed. If the Oversight Authority is only able to have oversight of the TDIF system, then it is not clear how a User gains resolution then remediation/redress when multiple digital identity systems are

potentially involved. Nor is it clear who pays for the associated cost in time and money to resolve any issues where this complexity arises.

At its worst, the complexity could lead to a User experiencing the Kafka-esque problem of ceasing to have an identity when the only way that the User can regain an identity is if they have proof of identity yet there is no one point to which they can turn to gain resolution. Depending on the circumstance, if requirements to submit a verified 'identity' become near universal, the User may require complete resolution within days in order to resume a normal life. Worse than that, if the failure leads to lifelong identity takeover, the User through no fault of their own may require lifelong and expensive assistance.

OAIC has neither the powers, processes nor the resources to resolve this quickly. An organisation like IDCARE is a not-for-profit facilitator/ombudsman, not a regulator with enforcement powers. The current proposals for the Oversight Authority appear more facilitative than anything more.

IIS recommends that the legislation is structured to ensure that the individual User is not left to navigate the complexity of such a multi-player system to find the source of the problem, gain resolution and remediation or pay any agent to do so. The legislation should ensure that the Oversight Authority or another entity acts on behalf of the individual to pursue such issues until they are resolved rather than the User the administrative burden.

Section 6 – Governance is covered in this section. As stated at the beginning of this Section, "Permanent governance arrangements are being developed to provide confidence for Users that their privacy and consumer safeguards are protected in the Legislation and are strictly enforceable by law". Credible governance from a User perspective will be one of the keystones to the TDIF framework gaining and retaining User trust. The leadership, powers and resources of the Oversight Authority and the other parts of the governance construct must be up to the task. As digital becomes ever more dominant in how individuals are to lead their lives, any compromise or loss of digital identity risks huge financial loss and enormous disruption of a life to the point of an individual User being rendered a 'non-person' through no fault of their own.

Section 6.4.1 – this section proposes that the legislation give powers to the Information Commissioner to allow them to enforce privacy safeguards in the system. This includes the safeguards in the Privacy Act, as well as additional privacy safeguards enacted by the Legislation. Set out earlier in Section 6, key elements of the governance structure include:

> "Rules will be enforced by the Information Commissioner, and the setting up of a new statutory officeholder responsible for the system and TDIF accreditation scheme. The responsible Minister will have power to issue Digital Identity rules and accreditation requirements and appoint advisory boards."

The Information Commissioner will simply not be able to enforce the Rules unless given significantly more powers and a significant increase in resources. Taking months to resolve

a complaint is totally unacceptable when a User's life is being harmed significantly on a daily basis.

IIS recommends that the legislation should only be introduced to Parliament if it is accompanied by actual appropriation of funds to the Information Commissioner that enable the Commissioner to enforce the Rules. If that is not possible, IIS recommends that the legislation should be accompanied a joint public statement to Parliament by the Minister responsible for the legislation and the Minister for Finance that commits the Government to provide specified additional funding. IIS further recommends that the legislation require the Information Commissioner to report directly to the Parliament with their view on the adequacy of resources provided including the initiatives that the Commissioner would undertake with additional resources.

Section 6.4.2 – This section sets out detail about the Oversight Authority and related advisory processes. That person "will be guided by expert advisory boards".

In the words of the Discussion Paper:

> "There will be at least one advisory board comprising of board members appointed by the responsible Minister, and the Minister may also establish other boards through issuing rules or other legislative instruments including:
>
> - a privacy and consumer advisory board made up of industry peak bodies, advocates and privacy commissioners
> - a technical standards board made up of entities participating in the system, as well as key experts from the public and private sectors
> - other strategic advisory bodies involving system Participants, state and territory governments, and other key stakeholders (including those that are not participating in the system)".

In effect, there would be no requirement on the Minister even to establish an advisory board with a privacy and consumer interest. The proposal goes on to indicate that any such board may be made up of "industry peak bodies, advocates and privacy commissioners", so that even there the voice of the advocate and consumer can be muted by powerful industry interests.

This aspect is particularly concerning. Ministers have repeatedly found ways to corrupt or weaken advisory bodies by who they appoint (or do not fill).

Options for a more influential involvement include a board on which User interests are represented having decision making powers over crucial matters such as the definition of identity and changes to accreditation rules, as well as the power to report directly to Parliament.

Another option is to appoint an independent Customer Service Commissioner, as NSW did on the establishment of Service NSW. Mike Pratt, the current Secretary of the NSW

Treasury was the State's first Commissioner. Here is how his Treasury CV describes what he did:

> "Prior to his role with Treasury, Michael was the NSW Customer Service Commissioner, where he revolutionised the way the Government delivers services - putting the people of NSW at the heart of service delivery in the establishment of Service NSW. He led major service reform across the NSW Government, chairing the NSW Customer Advisory Board - the responsible governance entity for the delivery of State Government services to the citizens of NSW."

The Secretary of the Department of Customer Service now performs the functions of the former Customer Service Commissioner. Unlike the original arrangement, this new arrangement removes the independent perspective of the Commissioner as somebody who is not also the service provider that the Commissioner is supposed to oversee.

IIS recommends that the legislation requires the creation of a consumer User experience, privacy and security board rather than leave its creation to the discretion of the Minister.

IIS further recommends that the composition of the consumer User experience, privacy and security board be spelt out in the legislation.

IIS further recommends that the legislation requires that User interests on the consumer User experience, privacy and security board be given dominant representation, on the basis that the board would be the only source of input to the governance of the system and that other interests have other channels.

IIS further recommends that the legislation give the consumer User experience, privacy and security board a more influential involvement in fundamental decisions about any of the Disallowable Instruments. Preferably, this would include the legislation giving the board a power of veto over crucial matters such as the definition of any core attributes in the TDIF rules and changes to accreditation rules. It would also include the power to report directly to Parliament.

IIS further recommends that complementary to the strengthening of the consumer User experience, privacy and security board, the legislation provide for the appointment of a salaried, senior, independent Customer Service Commissioner, with a role similar to the Customer Service Commissioner NSW created on the establishment of Service NSW.

Section 6.4.3 – This section sets out some more detail about independence and staffing of the Oversight Authority's office. It proposes that the Oversight Authority be independent statutory officer and not be subject to direction when performing the functions set out in the Legislation. The Oversight Authority would be a single person with support from seconded staff.

Other details are spelt out earlier in Section 6, including the proposal that the "Bill gives powers to the Minister to make rules and appoint an Oversight Authority as a statutory

officeholder to discharge the non-privacy regulatory functions and strategic operational functions given to that officeholder by the Bill."

[Figure 9] "also shows how the Oversight Authority is supported by an Office of the Oversight Authority staffed by public servants made available by an existing Commonwealth department or agency."

Setting up an Authority "staffed by public servants made available by an existing Commonwealth department or agency" seems to be emerging as the new preferred way to staff new regulators etc. IIS considers that this model has all sorts of questionable implications for an independent officer or regulator. Adverse implications include the head of the 'donating' department having a conflict of interest in deciding who and what proportion of the department's resources will be seconded from the department's other functions to the 'independent' body and potentially dual loyalties for the seconded staff. It may even compromise the independence of the Oversight Authority if it feels it is subordinate to or a 'Division' of the department.

A very close parallel was played out when the Abbott/Hockey 2014 Budget proposed to amalgamate the OAIC into the Human Rights Commission without separate resources because the head of the Human Rights Commission would decide how much of its resources to provide to the Information Commissioner. The Constitution prevented the Senate from amending the appropriation bills (i.e., the Budget legislation) which meant it could not object to this change in funding. However, the Senate was able to refuse passage of separate legislation needed to amalgamate OAIC into the Human Rights Commission. Eventually the government dropped the idea and OAIC remains separate from the Human Rights Commission with separate funding.

IIS recommends that the Oversight Authority be staffed by an Office separate from any Government Department even if back-office functions are provided by a department or another agency, similar for example to the OAIC. If such separation is not agreed, IIS recommends that the legislation explicitly state that the staff provided to the Oversight Authority are to be managed by and take direction only from the statutory officer holding the position of Oversight Authority. If separation is not agreed, IIS recommends that the legislation should be accompanied by a joint public statement to Parliament by the Minister responsible for the legislation and the Minister for Finance that commits the Government to provide specified additional funding. IIS also recommends that if the separation is not agreed, the legislation require the Oversight Authority report directly to the Parliament with their view on the adequacy of staffing resources provided including the initiatives that the Oversight Authority would undertake with additional staffing.

Section 6.4.5 – This section sets out the powers and functions of the Oversight Authority in more detail. Functions include:

- assisting with detecting and investigating cyber security, privacy breaches or fraud incidents

- seeking civil penalties against Participants
- coordinating responses to security incidents, disaster recovery and other incidents that impact the system, as well as issuing directions to Participants
- assisting and providing redress to victims of identity fraud perpetrated using the system.

"Assisting, seeking and coordinating" is not the same as taking the lead in resolving and ensuring resolution. IIS believes these roles need to be strengthened. From a User's perspective, the stakes can range from nuisance to ruin of the rest of their lives as has been attested by numerous individuals who have been subject to lifelong identity takeover. As such, some of the ways in which the Office of the National Data Commissioner (ONDC) has been established and empowered are not appropriate for the oversight of the TDIF.

The current remit of the Information Commissioner is also not sufficient for this task because the Commissioner's remit is limited more narrowly to the privacy aspects of the system. IIS considers that such a widening of the role of the Information Commissioner would inappropriately dilute the Commissioner's focus.

IIS recommends that the Oversight Authority be given powers beyond "assisting, seeking and coordinating". Such powers should include complete investigatory and enforcement powers: at a minimum similar powers as provided to the Information Commissioner and sufficient resources to apply them unflinchingly. IIS further recommends that if the powers of the Oversight Authority are not strengthened, the legislation identify which regulator will have those powers, functions, and resources.

IIS recommends that as recommended regarding other aspects of the resourcing of the system oversight, the legislation should only be introduced to Parliament if it is accompanied by actual appropriation of funds to the Oversight Authority or the other nominated regulator with power to resolve all User issues.

IIS recommends that if such an appropriation at the time the Bill is introduced is not possible, the legislation be accompanied a joint public statement to Parliament by the Minister responsible for the legislation and the Minister for Finance that commits the Government to provide specified additional funding. IIS further recommends that the legislation require the Information Commissioner to report directly to the Parliament with their view on the adequacy of resources provided including the initiatives that the Oversight Authority or the other nominated regulator would undertake with additional resources.

Section 6.6.3 – This section includes a statement that "Meta-data and logs of a User's previous Digital Identity may be linked to their current Digital Identity through a system-run process that is designed to identify a Digital Identity of the same individual". The implications of this are not clear. Nor is it clear what is meant by meta-data and logs. The system is not supposed to be tracking anybody, so the need for meta-data and logs is unclear. Once meta-data and logs are created, others will want access to it including law enforcement and national security interests even if that is not originally intended. This evolution follows like

night follows day, as was recently demonstrated by police seeking access to contact tracing information collected by QR code systems in at least three States, even after promises that this would not happen.

IIS recommends that the retained meta-data and logs be defined narrowly, that narrow limits be placed on which parties in the system can create them and that the length of time they are retained be restricted to a very short period such as the length of time to complete a verification and the associated service to which it leads.

IIS further recommends that similar to the provisions in the Privacy Amendment (Public Health Contact Information) Act 2020, the TDIF legislation be constructed in such a way that all uses and disclosures of meta-data and logs by any organisation in Australia or elsewhere, without exception, are unlawful beyond providing the identity verification service and running the system.

IIS further recommends that if the previous recommendation is not accepted, then any access by law enforcement and national security agencies only be allowed based on a narrowly constructed court order and that such access be subject to regular, detailed, independent, published audit and that criminal penalties apply to misuse.

Section 7.4.1 – The proposals here are absolutely vital. They are core propositions necessary to get away from inescapable digital oversight and the 'Digital God' problem. The propositions include:

> "It is proposed the Bill will provide individuals the right to voluntarily create and use a digital identity, including the right to deregister and not use a digital identity, at any time.
>
> It is also proposed the Bill will require a relying party using the system to provide an alternative channel to Digital Identity to enable individuals to access its services provided the relying party's service is not an essential service"

Unless genuine, feasible choice is available without coercion, then any 'consents' obtained to create or use a digital identity in the TDIF system will be invalid legally. Such a situation would also undermine significantly the trustworthiness of the system.

Section 7.4.3 – This section is one of the areas of the Discussion Paper that raises most concern. It reads in part:

> "It is proposed the Bill will prohibit Accredited Participants from collecting, using and disclosing information about a User's behaviour on the system, except to:
>
> - …
> - respond to lawfully made requests for information for an enforcement purpose (subject to the prohibition on speculative profiling for an investigatory purpose)"

There is also a lengthy description of an (excluded) 'investigatory purpose' in footnote 13, but at the end of the footnote is confirmation that "This means that speculative profiling will be prohibited for the above activities, but this does not prevent law enforcement accessing information in relation to suspected individuals under existing powers".

Law enforcement and national security access to User involvement in the system is simply unacceptable. Digital identity will soon be so central to leading ordinary life that it will be unavoidable, if it isn't already. If government wants TDIF based identity management to be widely trusted and used, it must promise privacy beyond the Privacy Act.

The logic is just the same as it was for the logic behind the Privacy Amendment (Public Health Contact Information) Act 2020 that protects the information collected by the Commonwealth COVIDSafe app. In that case, the question was whether or not government want people to trust the system to be used only for health-related purposes. The app was not constructed as a law enforcement or national security surveillance tool. The policy decision was that public health overrode all other considerations. That trust was paramount and the new legislation recognised that the Privacy Act as it stood before amendment provided insufficient protection. Since Australia Card, Australians have been especially suspicious of digital identity systems that have the potential for broad based surveillance. The Access Card proposition that finally failed in 2008 confirmed this is a long-lasting suspicion.

The logic is also the same for the law recently introduced to protect information collected by the WA QR code app. It is the same in the other States where police have sought access including in Victoria and Queensland. It is already prevented by law in New South Wales.

The government simply must decide whether or not it wants the TDIF as supported by the proposed legislation to be trusted and so used widely by the broader population.

At the very, very least if law enforcement or national security are to be allowed to access anything in the TDIF ecosystem, that access must be subject to production of a court order backed up by a credible assurances mechanism to monitor the process and outcomes.

On a related issue is the question of how this legislation will interact with other legislation including but not limited to the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020. If those pieces of legislation prevail, then the TDIF legislation potentially becomes totally ineffectual in protecting individuals from intrusions on one of the most basic aspects of leading a digital life: digital identity without surveillance of most aspects of their daily lives.

IIS repeats its recommendation that the TDIF legislation be constructed in a way similar to the provisions in the Privacy Amendment (Public Health Contact Information) Act 2020 where all uses and disclosures of information transacting in the system including meta-data

and logs by any organisation in Australia or elsewhere, without exception, are unlawful beyond providing the identity verification service and running the system.

IIS further recommends that the previous recommendation is not accepted, then any access by law enforcement and national security agencies only be allowed based on a narrowly constructed court order and that such access be subject to regular, detailed, independent, published audit and that criminal penalties apply to misuse.

Section 7.4.6 – This section proposes that the Bill require a User to consent expressly before an Accredited Participant authenticates and sends attributes to a relying party.

This is a welcome development but by itself insufficient.

IIS recommends that the legislation also explicitly require data minimisation (i.e., verification ONLY of the minimum relevant attributes necessary to complete the engagement between the User and the Relying Party) and that this be strictly enforced.

IIS further recommends further recommends that the relevant regulators including the Oversight Authority and the Information Commissioner must strictly and visibly enforce the proposed requirement that Relying Parties always offer alternatives that do not involve presenting a digital identity: otherwise the 'consent' would not be a legally valid consent.

IIS recommends that the legislation should only be introduced to Parliament if it is accompanied by actual appropriation of funds to the relevant regulators including the Oversight Authority and the Office of the Australian Information Commissioner that enable them to enforce the proposed requirement that Relying Parties always offer alternatives that do not involve presenting a digital identity and audit consent arrangements as implemented.

IIS recommends that if that is not possible, the legislation should be accompanied a joint public statement to Parliament by the Minister responsible for the legislation and the Minister for Finance that commits the Government to provide specified additional funding.

Section 7.4.8 – This section addresses the retention of data created by the TDIF system. However, no rationale for retention beyond the fulfilment of each particular verification is provided. The provisions of the archives legislation provide a very weak justification. Retaining such data for seven years means that a record of much of each User's life is recorded as a honeypot for all sorts of interests ranging from targeted marketing to law enforcement and national security, or worse a target for external malefactors. In the case of law enforcement this is explicitly acknowledged: "Data retained shall be for the purpose of maintaining the integrity of the system, which may include fraud or criminal investigative purposes".

Regardless of any possible justification such as maintaining the integrity of the system or resolving disputes that cannot be addressed by the parties from data they hold outside the system, seven years is many years too long.

By way of comparison, the Document Verification Service (now called IDmatch, https://www.idmatch.gov.au) used to retain the personal information it exchanged for very short periods of time. IIS recalls this included retaining the metadata for very short periods (days). IIS cannot verify the current policy on that website other than a vague answer in an FAQ that states:

> "We don't keep any personal information transmitted by our hubs to verify or identify you.
>
> As a general rule, we also don't permanently keep transaction data. We keep it for the minimum period required under the law and for auditing purposes."

IIS recommends that all parties in the system be required to securely delete verification transaction data including meta-data and logs within a small number of days from the completion of the verification.

Section 7.4.14 – This section allows some state and territory agencies to comply with the relevant state or territory privacy law rather than federal law.

This will lead to confusion among Users, especially when other parties e.g., Relying Parties are not state or territory agencies or vice versa. It could lead to a User finding that the one verification is covered in its different stages by different law. Users will find it difficult to understand which law applies and when and therefore not have a clear picture of their protections and right. One likely example is when the verifying party is covered by a different law from the relying party but there is a problem with the verification. The individual User is burdened with wading through such a legislative tangle especially if each party blames the other.

The Discussion Paper proposes that the legislation "require Accredited Participants to be covered by the Privacy Act. However, state and territory government entities will have the option of complying with a comparable state or territory privacy law. A state or territory law (other than for notifiable data breaches) will be considered comparable if it provides:

- protection of personal information comparable to that provided by the Australian Privacy Principles (APP) in the Privacy Act
- monitoring of compliance with the law
- a means for an individual to seek recourse if there has been a privacy breach."

This raises the question of who will decide whether a jurisdiction "will be considered comparable". Self-assessment by a jurisdiction is highly likely to lead to inconsistent decisions and possibly challenge. Taking the example of Tasmania where the regulator is the Ombudsman who can investigate and report but not enforce, there could well be different views on whether that constitutes provision of "a means for an individual to seek recourse". South Australia has a similar arrangement, but the relevant privacy principles are not

enshrined in law and the entity that provides the complaints handling service is a Committee that has no existence in statute nor has any statutory powers.

IIS recommends that the legislation follow the lead provided by the Privacy Amendment (Public Health Contact Information) Bill 2020 and apply the law to any participating state or territory agency including oversight and enforcement by the Information Commissioner.

IIS recommends that if that recommendation is not agreed, then the legislation provide for a 'one stop shop' solution where Users can have issues addressed and resolved relating to the impact on their lives of the TDIF system, regardless of which law applies. IIS further recommends that the one stop shop have the power to force the relevant parties and possibly regulators to work together until they can provide a response or remediation to the User.

IIS recommends that the legislation should only be introduced to Parliament if it is accompanied by actual appropriation of funds to the relevant regulators that enable them to deliver a simple and effective one stop shop to resolve User issues that arise from the application of multiple jurisdictions. If that is not possible, IIS recommends that the legislation should be accompanied a joint public statement to Parliament by the Minister responsible for the legislation and the Minister for Finance that commits the Government to provide specified additional funding.

IIS recommends that before a state or territory law is "considered comparable", the Oversight Authority publish and advertise a draft decision to that effect and invite submissions before a final decision is made in the form of a TDIF General Rule and hence that the decision be a Disallowable Instrument.

Section 9 – This section on a liability and redress framework is another vital cog in the design. However, such liability appears to be limited to non-financial liability. Section 9.4.1 states that:

> "The liability framework will involve two major elements:
>
> - mechanisms providing for non-financial redress for adverse outcomes that arise as a consequence of participating in the system, including for example, assisting with re-establishing a stolen Digital Identity
> - …"

Section 9.4 – provides further detail on redress.

Section 9.4.2 goes into detail about financial liability between Participants in the TDIF scheme (with "Participants" and "Accredited Participants" explicitly NOT including Users).

Section 9.4.3 exempts the Oversight Authority from any liabilities.

Section 9.4 seems to be the only place in the Discussion Paper that covers where and how Users can recover from any compromises. It seems to be focused mostly on fixing what went wrong directly, including re-establishing a digital identity with the Oversight Authority providing 'assistance' rather than actually ensuring things are fixed.

Indeed, it all seems very vague on redress for any wider (and potentially much larger) harm inflicted on the User as a consequence. At worst, harm can be a lifelong identity takeover inflicting huge financial loss and huge disruption of life.

The only reassurance in regard to those wider issues appears to be in the following statement in the Discussion Paper:

> "In addition, to ensure that Accredited Participants and Users have appropriate protection from identity fraud and cyber security incidents, Accredited Participants will be required to have adequate insurance arrangements in place as part of their accreditation requirements. This will ensure that there would be a reasonable degree of protection in place for all participants in the digital identity system."

This implies but does not explicitly state that the damage inflicted might be significant and way beyond simply regaining a digital identity.

During informal consultations, DTA staff indicated that the means of obtaining any redress would be up to the User to seek it through the courts. Such an arrangement becomes de facto a pathway only available to the well healed.

In short, the arrangements as described are too vague but to the extent that there is clarity, the means by which individuals can gain redress is highly unsatisfactory.

IIS recommends that the legislation designate the Oversight Authority or another suitably empowered regulator as investigator and decision maker regarding any financial and non-financial redress that a User may seek from failings in the system. IIS further recommends that the regulator be able to arrange and fund legal advice and representation in any court proceedings on behalf of the User.

IIS recommends that the legislation should only be introduced to Parliament if it is accompanied by actual appropriation of funds to the relevant regulators that enable them to provide redress to Users without financial cost to the User and minimum effort from the User.

IIS recommends that if the previous recommendation is not possible, the legislation should be accompanied a joint public statement to Parliament by the Minister responsible for the legislation and the Minister for Finance that commits the Government to provide specified additional funding.

Section 10.3.6 – Section 10 sets out the enforcement framework which seems adequate, if it is actually implemented with vigour. However, Section 10.3.6 is concerning. It passes the ball to OAIC without any mention of adequate funding.

Separate from funding issues, one of the key issues with OAIC is that it is its process do not facilitate rapid resolution. All the procedural fairness requirements make it a very long and drawn-out affair regardless of funding. The TDIF legislation needs to include new pathways for rapid resolution of problems with creating and using digital identities, at least from a User perspective.

IIS recommends that the legislation include procedures that enable the OAIC to provide speedy initial redress pending final decisions.

IIS further recommends that the legislation should only be introduced to Parliament if it is accompanied by actual appropriation of funds to the relevant regulators including OAIC that enable them to enforce the law as it applies to current or previous Accredited Participants and provide speedy redress to for all parties.

IIS recommends that if the previous recommendation is not possible, the legislation should be accompanied a joint public statement to Parliament by the Minister responsible for the legislation and the Minister for Finance that commits the Government to provide specified additional funding.

Malcolm Crompton AM Founder and Lead Privacy Advisor

Michael Trovato Managing Director and Lead Security Advisor

Information Integrity Solutions, Pty Ltd

July 2021