INFORMED MEDICAL OPTIONS PARTY
NO FORCED MEDICATION !
NO COMPULSORY OR COERCED VACCINATION !
NO FLUORIDE IN OUR WATER !
imoparty.com

27th October 2021

Peter Alexander
Acting Chief Executive Officer
Digital Transformation Agency
Australian Government
email: digitalidentity@dta.gov.au

cc: Hon. Stuart Robert MP

Informed Medical Options Party Submission
'Have your say on Australia's Digital Identity Legislation'

Table of Contents

1. Introduction – Consultation

This submission has been made in haste due to a lack of awareness, on our part, of this legislation. It appears that IMOP is not alone in failing to appreciate the existence and import of this proposed legislation. Despite the Digital Transformation Agency's (DTA's) insistence that public comment on the legislation has been solicited for almost six years, the proposed Act has received very little public attention. By contrast, it appears that key industry players have been widely consulted and engaged in the drafting of this legislation, as elements of it read like an industry white paper.

According to the most recent synthesis report, DTA consulted with approximately 300 stakeholders, hosted five webinars attended by 110 stakeholders and received 44 submissions: 36 from governments and industry, plus eight from individuals and consumer groups [1].

This is an extraordinary lack of public consultation for legislation that will ultimately affect 26 million Australians. This is a very serious concern and it raises questions about why the government would not want to engage citizens in a discussion on this topic.

On its own, this lack of consultation should be grounds for delaying the introduction of this legislation into Parliament. Compared to the 24/7 publicity and engagement accorded to the COVID-19 pandemic by government funded campaigns over the past 20 months, this legislation appears to have proceeded in stealth mode.

2. Implications of a Lack of Consultation

In our opinion, the absence of significant community input into the legislation is reflected in the way in which users are positioned within the system. The whole Act has been framed to sustain the current business models of Silicon Valley tech giants which are predicated on surveillance and data-extraction. Under the proposed legislation, system participants will be able to treat users as system products – the same way that Facebook treats its users.

The proposed Digital Identity System makes provision for system participants and reliant parties to efficiently authenticate system users. In doing so it recognises the value of identifying information, but it comprehensively fails to provide any mechanism for justly or equitably sharing the value of that information between system participants and system users. Such a design will only entrench and perpetuate the worst features of our existing digital business models while failing to realise the economic potential of Web 3.0 innovations. Over time this fact will become apparent to system users and may eventually result is widespread distrust of the system and a search for alternatives.

This draft legislation fails to capitalise on many of the user-empowering innovations that are beginning to comprise the next version of the web. If there had been a greater public awareness of this legislation and more community consultation, it is unlikely that the legislation would have remained in its current form.

3. IMOP Concerns

1. The proposed legislation is based on an outdated framework for managing Identity.
2. It relies on privacy law as its primary form of consumer protection rather than structural design.
3. It contains no provision for recognising the property-rights of data originators.
4. It offers no protection from the data-harvesting business models of Silicon Valley platform providers.

4. Legislative Intent

Australia has a long history of failed national identity schemes starting with the Hawke government's proposed Australia Card in 1985, which led to a double dissolution of Parliament. This was followed 10 year later by the Howard government's Access Card which was eventually abandoned by the Rudd government in 2007. There are well documented reasons for these failures, with trust being a central issue. Sadly, this current project is following a similar trajectory.

One of the principal reasons Australians are suspicious of national identity schemes is that they see them as empowering governments at the expense of citizens. The current legislation is no exception. The benefits listed by the DTA as arising from this proposed National Digital Identity scheme are principally benefits accruing to government and industry. References to 'citizen' or 'user' centricity in the legislation reflect a very shallow interpretation of these notions – focusing more on the user experience than genuine economic empowerment.

A favourable reading of this legislation would conclude that it has been proposed by government for government. An unfavourable reading would suggest that it has been proposed by government to facilitate an unhealthy merger of state and corporate interests – with everything that entails. This interpretation of the draft legislation goes right to the heart of the trust issue. IMOP accept the proposition that some form of robust digital identity is central to our successful development as a nation in the 21st Century, however, attempts to regulate digital identity in a manner that empowers data-harvesters and brokers at the expense of data-originators will result in distrust of the proposed system and continual attempts to circumvent it using the plethora of alternative tools available, such as trust-less blockchains (amongst many other options).

IMOP's concern with the intent of this legislation is that it reflects government and industry interests almost exclusively and that it relegates users – the citizens of Australia – to the position of passive data-subjects.

5. A Flawed Framework for Digital Identity

The proposed Trusted Digital Identity Framework is predicated on the idea that individuals can re-use authentication information across multiple contexts. This idea has been something of a canon in the digital identity space ever since Kim Cameron first published his Laws of Identity in 2005 [2], but despite its popularity, the idea has met with very limited success. Billions of dollars have been spent on public and private projects which attempt to streamline user authentication by means of interoperable identities, but these initiatives have resulted in more failures than successes. On top of this, trade in stolen data continues to grow in spite of ever-increasing cyber security expenditure and tightening governance in traditional identity frameworks. The existing credentialing paradigm is ripe for transformation, and new technologies to address these problems are already operational, such as peer to peer engagement using Public Key Infrastructure. This begs the question, why is the Australian government proceeding with an identity architecture that is not best practice? IMOP's concern is that this is occurring due to the outsized influence of global tech industry players who are keen to entrench their existing privileges within a legislative framework – insulating themselves from disruptive competition.

6. Problems with Trusted Digital Identify Framework (TDIF)

One of the central problems of TDIF is that it has no mechanism for managing liability in the event of a large-scale system failure.

This begs the question, why is the Australian government proceeding with an identity architecture that is manifestly not best practice? Especially when new technologies to address these problems are already operational. such as peer to peer protocols and Public Key Infrastructure amongst many other tools.

IMOP's concern is that this is occurring due to the outsized influence of global tech industry players on the development of this legislation. This problem is exacerbated by a lack of community engagement. IMOP believes that the current legislation will stymie innovation and economic growth in the Web 3.0 economy and entrench the data-extraction business model of existing tech giants within a legislative framework – insulating themselves from disruptive competition.

7. An Alternative to TDIF

In recent years Digital Identification architectures have moved away from the concept of unified identity to reliance on contextual trustworthiness. Contemporary verification techniques rely on decentralised protocols and algorithmic and cryptographic credentialing tools to prove trustworthiness, not identity. This is entirely different to the approach used in traditional banking, yet the digital finance (DeFi) industry is growing exponentially using these tools to govern trusted and untrusted peer to peer transactions.

Critically, these new ways of identity management do away with the need for centralised identity and identity providers such as the ATO or Australia Post. Instead, what is evolving is an emerging ecosystem of data controllers, attribute providers, information brokers and value adding data processors, all meeting the needs of reliant parties.

Some of the failings of federated identity systems is that they rely on positive verification methods, as opposed to negative verification. They encourage over-sharing of identity information and they also make no provisions for anonymous interactions. As a result of these limitations, a whole new class of identity management solutions has arisen, relying on decentralised protocols and decentralised IDs.

Decentralised protocols generally rely on Distributed IDs (DIDs) as the type of identifier that enables a verifiable, decentralised digital identity verification on a network. A DID allows any person, organisation or thing on the web to identify itself in whatever way the controller of the DID decides to identify itself. For each transaction, the ID owner decides what attributes they will use to identify itself. The controller of a DID can prove control over the identity using any identifying attribute appropriate to the transaction and this can be verified independently of any centralised registry, identity provider, or certificate authority. DIDs are URIs that associate a DID subject with a DID document allowing trustable interactions associated with that subject. Identifying documents can express cryptographic material, verification methods, or service endpoints, which provide a set of mechanisms enabling a DID controller to prove control of the ID. Once this is done, network protocols enable relying parties to engage in trusted interactions with the DID subject.

Decentralised protocols are sets of rules or procedures used by electronic devices to regulate the transmission of data between themselves. In order for computers to exchange information, there must be a pre-existing agreement as to how the information will be structured, sent and received. These can be thought of as packets of software code. Decentralised protocols allow client and host nodes to combine and create a secure private network. Such networks can scale from two nodes to millions of nodes.

Within this network, trusted exchanges can occur through the use of algorithmic and cryptographic keys. On such networks, externally verifiable IDs may not be required. The relationships between nodes on the network are trustworthy since they are controlled by secure keys. Trust is not a feature of the identities transacting on the network but rather it is a feature of the network itself. This allows participants to interact with each other anonymously but still in a secure way. It also allows for software governed micro-contracts (smart contracts) to be put in place governing every aspect of any relationship. Such contracts can provide for micro-payments to be made bi-directionally. This is a much fairer and more just system of online interaction than we have today. It is also profoundly disruptive to the existing business model of the internet.

The key to all of this is verifiability. A key property of Web 3.0 is its ability to prove the veracity of claims algorithmically without reliance on any centralised authority. This seemingly simple feature unlocks extraordinary opportunity for equitable collaboration and scaling. It is about as revolutionary as the hyperlink. Web 3.0 will bring us a fairer internet by enabling the individuals to own and control who profits from their time and information. If the web is allowed to develop without undue interference from governments, this model of operation will likely replace the exploitative business model of our existing web over time. This would see the end of centralised platforms like Google, Facebook and Amazon, which make obscene profits at everyone else's expense, and the rise of a sustainable economy-wide eco-system of digital businesses.

8. Anonymising the Online Experience

As pointed out above, anonymity is central to our sense of identity. It may seem counterintuitive, but evidence that people take anonymity seriously can be found in the phenomenal growth of crypto-currencies and the whole Web 3.0 movement, which has many of the brightest technology minds in the world engaged in it, including Tim Berners-lee. Until the rise of COVID tracking apps, Australians were free to move about their country without having to identify themselves to anyone, unless suspected of a crime. This is a prized freedom and one that does not exist in authoritarian regimes. Our recent loss of this freedom says much about our current political climate and it augers very poorly for legislation like TDIF.

9. Positive vs Negative Verification

In most transactions that people have with each other, negative identification is sufficient to interact securely. For example, a licenced venue only needs to know that someone is over 18 years of age to serve them a drink, nothing else. This can easily be established through negative verification. No positive identification is required. Many commercial transactions can proceed on a similar basis.

The proposed TDIF relies on tiered levels of positive identification – a feature that introduces a high level of systemic risk into the proposed legislative framework.

As the digital and physical worlds begin to merge together, as is happening with the evolution of the internet of things (IoT), a reliance on positive forms of identification means that there will be quite literally nowhere that a person could hide from view if a body with sufficient technological reach wanted to locate them. Such a capability has been the long-cherished dream of governments everywhere, even benign ones, but it represents perhaps the most significant risk to human freedom and autonomy that humanity has ever faced. Imagine such a power in the hands of a foreign government or an unaccountable global corporation?

In its current form, this TDIF appears to be relatively benign legislation, but like most legislative endeavours, there is a risk of significant scope creep over time. Digital identity represents a perfect fusion of government and corporate interests. Nothing fuses the two groups more neatly or tightly than the ability to monitor, and even control (nudge), every data-subject on their network.

10. A Government Trust Deficit

In recent years there have been countless revelations of governments and private corporations illegally compromising the privacy of individuals. Yet almost no one has been prosecuted for these breaches. Edward Snowdon's revelations regarding the activities of the US NSA and its 5-Eyes partners (including Australia) were met with passive outrage. There were no policy changes, legislative interventions or even prosecutions. In Nov. 2020 Australia's intelligence agencies were caught 'incidentally' collecting data from the country's COVIDSafe contact-tracing app during the first six months of its operation [3].

On top of these executive breaches of citizens' rights, we see Premier Daniel Andrews instituting semi-permanent states of emergency and legislative exception in Victoria which, he claims, already have precedent in New Zealand – a precedent which could easily extend across states within Australia. Under Andrew's proposal, 'health security' calibrated to so called 'worst case scenarios' will become the model for future governance in his state. These are dangerous developments and legislation like the TDIF is creating instruments for biosecurity management that could be easily co-opted to nefarious purposes. It is for this reason that IMOP support non-centralised, anonymity preserving, decentralised identification solutions, not TDIF.

In 2018 the Australian Government passed the Identity-matching Services Bill 2018. Like the proposed TDIF legislation, this Bill contained numerous 'nominal' protections for citizens but loose drafting left a great deal of room for the misuse of biometric personal data regulated by this Bill to be re-purposed for law enforcement purposes. This resulted in biometric data collected from citizens for the purposes of facial verification in things like driver's licences and passports, being repurposed by law enforcement for a broad-based one-to-many search, surveillance and matching system. This issue goes to the heart of the trust issues Australians are increasing encountering when interacting with governments. Information that they were assured would be 'safe and secure' ultimately ends up in the hands of law enforcement and used against them in warrantless (unauthorised?) forms of surveillance

11. A Bill of Digital Rights

In Australia we have no Bill of Rights for citizens. This has often been considered as a serious deficit of our democracy. Notwithstanding, no such Bill is likely to be proposed any time soon. However, we could develop such a Bill for cyberspace. An Australian Bill of Rights for Cyberspace could turn out to be a liberal folly or it could become the basis for one of the most competitive and productive digital economies in the world. Critically, any such Bill would be predicated on strong principles of justice, including distributive justice, respect for autonomy and respect for property. Importantly, as labour in all its forms, becomes less central to our economy, some form of distributive justice will become a necessary feature of our society going forward.

This will require a move away from the current rent-seeking model of the internet and a move towards a more democratic distribution of value through the value-nets that comprise our evolving hybrid economy. Such a Bill may even contain provisions to mitigate the power-law distributions of wealth and influence that result from massive network-effect by insulating physically localised businesses from the predations of global technology companies. For example, ride-sharing and food delivery services in Wollongong may be prohibited from utilising global platforms to offer their services, instead relying on local developers to build local versions of on-line booking platforms.

12. Governance as the Solution

Without safeguards, digital identity opens up the possibility of serious misuse. Even with a full suite of ‘supposed’ safeguards, recent history shows that unpunished abuses of personal information are almost a certainty. With digital identity, the shop assistant selling you alcohol might see less of your personal information than they may otherwise have if you had handed over your licence but, because this transaction confirms who you are, your purchase information could be on-sold to interested parties, such as your health insurer (affecting your premium) or DHS (affecting your cashless debit card payments). The DTA has advised that it is currently considering establishing an oversight authority, oversight rules, or both, that would seek to prevent the on-selling of data, harvested through digital identity verification. This sort of oversight is fatally flawed. If the ability to geo-locate, track and control every person through physical space in real-time exists, it is only a matter of time before someone, either a government, a corporation or a bad-actor uses that information for their own ends. The most secure form of governance available is to design anonymity into the system using the Web 3.0 protocols detailed earlier so as to ensure that it is technically impossible for abuses of privacy to occur.

13. Privacy is not the Answer

In 2018 Fergus Hanson published a report [4] where he suggested that the government should conduct a “root-and-branch review of how citizen protections can be made fit for purpose in the 21st Century and of opportunities to take advantage of digitisation to simplify rules created for our paper-based society." He suggested that this should include minimum security baselines for stored data applying to both government and the private sector. He suggested some useful ideas such as "an accessible log recording each occasion someone’s personal information is accessed by any arm of government or the private sector and a one-click process for contesting unauthorised access."

These are well intended ideas but privacy is a poor shield from the deep structural problems associated with digital technologies. 'Privacy' rather than 'justice' has become a mantra. While every tech company in the world is prepared to make public commitments to privacy, few of them will address the issue of data justice, i.e. rebalancing the massive asymmetries of informational power that exist between natural and corporate persons. Nor are any of them interested in recognition of personal data sovereignty, i.e. enduring, exclusive, alienable rights vested in data subjects (you and I) vs those assigned to data harvesters and processors.

As digital technologies remove one frontier after another of insight into the lives of natural persons, we find technology companies and governments are increasingly relying on intellectual property rights, trade secrets and national security to exclude any insight into their workings. This is resulting in a creeping structural injustice where we have two classes of persons under the law: the class of natural persons who have few legal defences against the onslaught of predatory data harvesting and no rights to exclusive ownership of their personal information, and the class of government and corporate persons (and their agents) who enjoy legal protection from almost all forms of scrutiny and exclusive, enduring, alienable rights to any and all data they harvest from others. Clearly, the concept of 'privacy' is serving two masters in this debate. This conflict makes it a weak tool for protecting the rights of natural persons. It would be much better if we relied on the far more robust legal principle of 'justice' for protection against the predations of Big Tech.
Of course, such a change in policy is not going to happen so long as corporations are setting the agenda. This is why a massive engagement effort by the government, comparable to the coronavirus response, is required if we are to successfully transition to a just and productive digital future.

14. Digital Identity as a Juridical Entity?

One possible drawback of identity schemes like the TDIF is that such schemes may, in time, inadvertently or otherwise, instantiate digital representations of natural persons as juridical persons in their own right and not as mere tokens or representations of their natural counterparts. A juridical person is a non-human legal entity, authorised by law with duties and rights and is recognised as a legal person and as having a distinct identity. This would be an extraordinarily disempowering development for natural persons but not entirely out of the realms of possibility. Some consideration of the unintended consequences of this legislation needs to be considered and the best format to do that is via well advertised public consultation forums.

While this is still an emergent idea, there is a possibility that a Federated Identity, animated by an AI tool and tasked to make minor decisions and authorise minor commercial transactions on behalf of its natural owner, could qualify for recognition as a juridical person with agency and interests in its own right [5].

15. Digital Identity as Property?

Some lawyers have theorised that digital identities may constitute a form of property which can, and should, be legally protected. Research has shown that digital identity can be interpreted as a form of property which is capable of being stolen and criminally damaged. Australian lawyer Clare Sullivan argues that an individual has the right to an accurate, functional digital identity and shows that this right exists in addition to the right to privacy. She maintains that, considering the essentially public nature of identity, the right to identity provides better, and more appropriate, protection than is afforded by the right to privacy. She asserts that the importance of the right to identity in this context has been obscured by the focus on privacy [6].

16. The Internet of Bodies

The intent and consequences of this legislation make possible the dystopic vision of Bruce Sterling who the world wide web is continuing to evolve at breakneck speed. New innovations such as the Internet of Things and the Internet of Bodies are evolving all the time. All of these innovations are heavily reliant on data - with personally identifying data being the most valuable. IMOP is concerned that the proposed TDIF legislation is not addressing the fundamentally predatory nature of the business models used by the large platform operators, Google, Amazon, Facebook, Apple and Microsoft, and that failure to do this is a massive oversight in the legislation. Claims that the TDIF verification procedures will protect the data of Australian citizens as they identify themselves scores of times a day on public transport, in shops, on the phoneand on-line are hollow to say the least. The large platform providers have thousands of computable attributes applying to each of us and can easily identify us in situations where our personal data happens to be unavailable to them. They do this by means of reverse induction AI algorithms or by using third party correlations which can provide very high levels of identification certainty. The challenge of the internet at this time in history is not the one being addressed by the TDIF legislation.

17. References

1. https://www.digitalidentity.gov.au/have-your-say/phase-1-digital-identity-legislation/digital-identity-legislation-synthesis-report
2. https://www.identityblog.com/?p=352
3. https://beta.documentcloud.org/documents/20416358-report-to-oaic-may-nov-2020-covidsafe-app#document/p2/a2005851
4. https://www.aspi.org.au/report/preventing-another-australia-card-fail
5. https://library.oapen.org/handle/20.500.12657/33171
6. https://library.oapen.org/handle/20.500.12657/33171