Lockstep Consulting
11 Minnesota Ave
Five Dock NSW 2046
AUSTRALIA

29 December 2020

Digital Transformation Agency

By web submission.

Proposed Digital Identity Legislation v2

Lockstep Consulting thanks the DTA for the opportunity to make this submission on the proposed Digital Identity legislation.

I am happy for the submission to be made public, including any Personal Information herein.

Executive Summary

The challenges of digital identity are as old as the Internet itself. I will not expend any effort going over this well-trod ground, except to stress that despite its great urgency, digital identity has been *by far* the slowest moving field in all of cyber security. It is beyond time that we look for fresh perspectives so that progress finally meets expectations.

Australia has been at the international forefront of privacy, authentication, e-signatures and what is now called digital identity since the 1990s. Australian governments were among the first in the world to deploy and regulate public key infrastructure, electronic conveyancing and digital driver licences, to name a few technologies. We passed the Federal Privacy Act in 1988 and have worked hard to keep multiple layers of privacy statutes reasonably current. We are now amongst the very first to legislate for open banking through the Consumer Data Right. Our state government digital services are world-renowned. Our private sector has spawned many innovative companies and pioneers, and our interdisciplinary cyber academics are among the very best. Australia knows how to do digital.

Further, Australia has established several pieces of critical cyber "infostructure" including the DVS, with the FVS expected to see similar success. We have a solid, technology neutral regulatory regime for e-commerce. There are many vigorous cyberspace institutes, Cooperative Research Centres, security centres of excellence, cross-disciplinary collaborations and think-tanks. These interlocking hard and soft innovations are all helping give shape to the infostructure of the future economy.

We now have a rare opportunity to break through the challenges of fidelity and provenance that plague cyberspace and, with a gentle course correction, deal with a bigger and yet more manageable problem than digital identity, namely the quality and reliability of data itself.

We should take heed of the global identity industry's move away from "identity". The hottest topics now are verifiable credentials, digital wallets, provenance, proof of possession, proof of control, personal hardware and embedded cryptography. The orthodoxy of Federated Identity may have had its day; there are still no commercially sustainable free market "identity providers" anywhere in the world. We should be especially wary of layering new architectural novelties on top of a tired old world view, when the identity problem at its heart is not technological.

All the same, the identity industry has built a powerful toolkit of standards, protocols, technologies and managed services. These are ready to be applied to a spectrum of urgent problems adjacent to identity: fraud in general, counterfeiting, synthetic identities, imposters, fake news and Deep Fakes. We have the tools and the infostructure is just around the corner to tackle fakes, fraud and online manipulation.

With this vision in mind, I will answer most of the consultation questions, with the hope to illuminate a bigger purpose for our digital identity methods. My proposed course correction will be gentle; it will retain almost all of the identity building blocks that so many have worked on for so long, in Australia and internationally. And I believe the correction represents an easier way forward. Digital identity has been such a fraught area, bogged down by controversies, complexities and misaligned expectations. By reframing digital identity as a matter of data protection in more general terms, we would stay out of the risk management ploys and business affairs of others, preserve today's many ways of credentialling and transacting, and be seen to focus on more objective security outcomes.

About Lockstep and the author

Lockstep (est. 2003) is an independent research and advisory group dedicated to digital identity, privacy and data protection. Lockstep Consulting has been engaged to provide research, analysis and advice for (among others) the U.S. National Strategy for Trusted Identities in Cyberspace (NSTIC), TDIF, the Australian Payment Council, Project Gatekeeper, the FIDO Alliance, the NSW Digital Driver Licence, Service NSW, Service Victoria, SA Health, the AGD's National Facial Biometric Matching Capability, Medicare Australia, the National Authentication Service for Health (NeHTA), the Open Identity Foundation, IBM's blockchain identity service, Evernym and the Sovrin Foundation.

Sister company Lockstep Technologies conducts breakthrough R&D on personal data protection and attributes management. We were contracted over 2016-19 by the U.S. Department of Homeland Security (DHS) through the Kantara Initiative to develop a mobile attributes wallet for first responders. Lockstep is the only Australian company to be awarded a DHS cybersecurity commercialisation contract.

Further background details are attached.

Preliminaries

Before looking at the consultation questions, I would like to set the scene with some contemporary observations of the state of the art in digital identity worldwide.

The trend away from "identity"

It is ironic that as Australia drafts legislation for digital identity, the digital identity industry continues its steady move away from "identity" as the organising principle for better authentication. Experience shows that federated identity — at the grand cross-sector scale envisaged by the *Laws of Identity*, NSTIC and GOV.UK Verify — is easier said than done [1]. Identity means different things to different people; we have yet to find a "lowest common denominator" for digital identity. On the other hand, on a daily basis we transact using numerous commonly understood attributes and data items. More on this later.

the best efforts of a great many, there is still no sustainable free market digital identity ecosystem anywhere in the world. If digital identity is such a good idea, we would have seen stable commercially successful "Identity Providers" emerge by now of their own accord in Canada, New Zealand, U.K., the U.S. and Australia. Even with tens of millions of dollars injected into broadly-supported public-private partnerships, IdPs have not succeeded. Instead, each of these familiar jurisdictions has a history of failed and struggling identity businesses and schemes. Lockstep stresses there is nothing wrong with failure as such, so long as we learn from it. The lesson is that identity cannot be "provided" as if it were a good or a service.

All the major identity industry initiatives are moving away from "identity". The hottest technical standards are the nearly complete *WebAuthn* and *Verifiable Credentials* protocols from W3C. And these are about *authentication* and *credentials*, not identity. The FIDO Alliance — arguably the best supported and most impactful initiative this sector has ever seen — pointedly *never* sought to solve "identity". One of the most influential Self Sovereign Identity (SSI) frameworks, the Sovrin Foundation, is proud of the fact that they do not deal with any artifact called 'identity'.[1] Many of the well-known *identerati* have told me informally that they regret how the term "identity" has become rusted on, because there is still such ongoing disagreement and distraction over what it means.

Even if it persists with this increasingly meaningless label, the digital identity industry in effect is dropping down a level, leaving aside abstract and relative visions of identity, and focusing instead on concrete objective attributes, with an emphasis on agency, provenance, proof of possession and security of the technical authenticators. **In Australia we have the opportunity to embrace this trend and build upon it with a gentle reframing of digital identity as a special type of data. We can re-use almost all of the existing IDAM standards, protocols and technologies to protect tightly defined attributes instead of broadly framed "identities". We can clear up the terminology and tighten the associated expectations, simplify the operational concepts of the participants, and make better progress on really urgent digital security challenges.**

[1] See "What is SSI?" by Phil Windley, Chair, Sovrin Foundation, June 24, 2020 at https://www.windley.com/archives/2020/06/what_is_ssi.shtml. According to Windley — who is one of the leaders of the Self Sovereign Identity movement, and a co-founder of the famous Internet Identity Workshop — in SSI systems "there's no artifact called an 'identity.' The primary artifacts are relationships and credentials. The user experience involves managing these artifacts to share attributes within relationships via credential exchange."

Reviewing the priority use cases and the real challenges

There would be broad agreement that the priority use cases for digital identity in Australia include:

- "KYC Once" (the long awaited ability to take the fact that a given set of EOI documents have been accepted for KYC and re-use that fact — nothing more and nothing less — across more than one financial institution or AML organisation)
- proof of age at licenced venues and online outlets, and
- mitigating the theft and abuse of government issued credentials (most notably Medicare card details which continue to appear for sale on the Dark Web).

We could well add to this list the highly topical demand for trusted digitised COVID-19 test results and proof of vaccination [2].

The real challenge in all of these use cases is to make sure that received data about people and entities is reliable, that Relying Parties can tell where data has originated, and they can be sure it's been presented with the proper agreement or involvement of the Subject.

We have plenty of sources of truth "IRL" and plenty of rules and systems governing them, including how any important credential is created, who is entitled to claim it, who should rely on it, and terms & conditions for use. The overwhelming problem in the digital realm is not "identity" as such but rather the conversion of real world credentials from analogue to digital forms. As things stand today, we cannot be sure of someone's age online, or their Medicare number, or even whether or not they are a dog.

Learning from verifiable payments data

While so much uncertainty plagues most personal data online, note carefully that we are increasingly able to be sure of credit card numbers. In *Card Present* transactions, cryptographically verifiable account details are secured between a chip card or mobile phone and a merchant terminal. In *Card Not Present* transactions, steady progress is being made on protecting the provenance of these same details as well.

What can digital identity policy makers and architects learn from the payment card experience? I suggest that chipped credit cards are the first instance of what we now call Verifiable Credentials. A credit card chip (whether it is embedded in a card or else uses the secure element of a mobile device) contains account information digitally signed by the issuing bank, to make the information essentially immune to counterfeiting. In each transaction, the purchase information is digitally signed in the chip so it cannot be intercepted, tampered or counterfeited. The digital signature is protected by a hardware Root of Trust in the terminal equipment, proving that the customer's chip is itself genuine. In summary, embedded cryptography conveys the provenance of the issuing bank, the chip and the payment scheme, assures the integrity of the customer account data, and ensures the presentation of the data cannot be faked.

This level of verifiability has been standard in payment cards for over a decade; it is nearly ubiquitous worldwide and across all retail payments. Moreover, it is thoroughly *consumerised*; people expect to be able to tap a card or wave a phone, enter a PIN in some circumstances, and have payments flow seamlessly.

The big question for digital identity going forward is this: Why not replicate the very same convenience, provenance, fidelity and security that consumers enjoy with payments? Why don't we equip Australians with the ability to move their credentials and personal data around with the same ease and security as a payment device? It would be easy.

General comments on the Digital Identity system and legislation

The Digital Identity system architecture

The proposed Digital Identity system builds on a relatively neutral framework (namely TDIF) but has morphed into quite a detailed architecture. The system embodies a technical world view that identity data and attributes are always presented in a particular way: retrieved in real time from "Identity Providers" and served up to Relying Parties via an intermediate exchange. There appears to be no way in the proposed scheme for individuals to deal directly with Relying Parties peer-to-peer, with credentials that might, as an alternative, be baked into personal devices just as credit cards and transportation tokens carry secure customer data. The proposed Digital Identity system is highly centralised, which will put it at odds with many contemporary thinkers. Do all attributes presented by Subjects to Relying Parties need to run through the IdX? This means that obtaining any anonymous attribute requires first an identification process and second the discarding of the identification details.

Lockstep cautions that the novelty of intermediated credential presentation brings risks. The novelty in and of itself makes legal analysis, risk assessment and contract negotiations difficult, for there are few precedents for this new way for Relying Parties to manage identification risks [1]. I will pick up on this issue at a few more points below.

Building role of Identity Exchange into the Digital Identity ecosystem also creates a variant on the risk of vendor lock-in. If accreditation of government-sanctioned digital identity solutions in Australia centres on this one particular architecture, and if there is no way for alternative solutions that don't feature the IdX to be considered for accreditation, then we will see a technological monoculture arise. If DTA is concerned about fostering innovation — a topic that crops up elsewhere in the discussion — then I hope that the architecture does not become too rigid, and that the central IdX is not enshrined.

Addressing the consultation questions

3.1. Purpose of the Legislation

1A) Are [legal authority, privacy protections, governance] relevant matters which should be included in the Legislation?

1B) Are there additional matters which should be considered?

Yes. See more details throughout our submission.

3.2. Structure of the legislative framework

2A) What matters covered by the TDIF should be incorporated into the primary legislation?

2B) What matters covered by the TDIF should be incorporated into Operating Rules?

2C) What matters covered by the TDIF should remain as policy?

We do not have clear cut opinions about these matters.

3.3. Scope of the Legislation

3) Is a publicly available 'Digital Identity Participant Register' an appropriate mechanism to communicate who will be covered by the Legislation?

Not entirely. Lockstep suggests that more than a register is required.

As transactions become more and more digital, we increasingly need to rely entirely on machine-readable electronic signatures and credentials. This includes machine-readable accreditation status of a credential. For instance, when a pharmacist receives a prescription electronically signed by a doctor, the pharmacist's computer system should be able to verify the signature, verify the status of the doctor, and verify that the doctor's credential has been issued by an accredited Digital Identity Participant.

This last step might be done by connecting to the suggested Digital Identity Participant Register and checking that the credential issuer is listed. If DTA went down this path, there would need to be specifications for interfaces and availability, and policies for handling situations such as outages. There also needs to be audit trails so that the historical fact of a credential lookup remains available, and record keeping so that the past validity of expired credentials may be reviewed.

4) Are the proposed obligations on relying parties … reasonable? Should there be any additional obligations?

Relying Parties should certainly be obligated to abide by system rules. Given the interconnectedness of the systems, these obligations might conceivably extend to software and cybersecurity.

It would also seem inevitable that if the Digital Identity system promises double blinding (of where identities are being presented and where identities and attribute come from) then Relying Parties will have to execute legal contracts with the system operator, embodying terms & conditions. There could be unforeseen costs associated with the sorts of contracts, and maintenance of the contracts in the face of any ongoing changes to system rules as the system evolves.

5) Are the concepts outlined above appropriate to include in a definition of 'Digital Identity' for the Legislation? Are there any additional concepts that should be included?

We are concerned that co-opting a common industry term "digital identity" and giving it a special meaning in the context of federal legislation might be counter-productive. Merely capitalising a phrase that is in widespread use in order to connote a special meaning can be confusing.

The legislation papers tend to use the term "Digital Identity" in the singular and without qualification; for example:

> *Over 1.7 million Australians and 1.2 million businesses already use Digital Identity to access over 70 government services*
>
> *using Digital Identity will help new business owners to save time and money*
>
> *Before Digital Identity, Alex had to …*

This style of usage seems almost like a branding exercise. If technically "Digital Identity" in capitals is an "electronic representation of an individual whose identity has been verified using the system" and if the "system" is that being legislated, then it's an exaggeration to count *myGov* in the 1.7 million Australians and *AUSkey* in the 1.2 million businesses, as these authenticators came from different legacy infrastructures.

6) Does the Legislation need to include a definition of Digital Identity information, or is it preferable to rely on the definitions of personal, sensitive, or protected information in other Commonwealth Acts?

"Digital Identity Information" is for the most part, just a special class of Personal Information (except for interesting edge cases like anonymous proof of age or strong pseudonyms). Existing definitions from privacy and other data protection statutes adequately cover the linguistic space.

3.4. Financial sustainability of the system

7) What factors should be considered in the development of a charging framework for the system?

In a traditionally light touch regulatory environment, I can't imagine how Identity Providers could be barred from charging — one way or another — for identity services. We draw a parallel with the deregulation of credit card surcharges and the way merchants now often bring out the merchant services feed explicitly in their customer bills. If government truly believes in a mainly market-driven digital identity environment, then it should probably refrain from saying much at all about charging.

3.5. Liability

8A) What factors should be considered in the development of the liability framework?

We feel that a critical missing piece is the structural change to liability arrangements that comes with Participants in effect *outsourcing identification* of their users to an arms-length data provider. What's more, the outsourcing arrangement is mediated by an entirely new type of organisation, the Identity Exchange. Lockstep's experience with numerous other identity federations is that contract negotiations stall when Relying Parties, Identity Providers and the system operator get together and begin to come to grips with the changes in risk is managed.

It is conventional wisdom that *businesses cannot outsource "risk"*, but since the express objective of Digital Identity is to reduce the risk that people face in dealing with each other digitally, there needs to be greater clarity about the liability that different participants really do accept.

8B) In what circumstances should Participants be held liable under the liability framework?

8C) What remedies and/or redress should be available to aggrieved Participants and Users for loss or damage suffered as a result of their use of the system?

8D) What other best practice mechanisms and processes should be considered to support Users when things go wrong?

Lockstep is not able to comment with confidence on these matters.

4.2. Privacy

To set the scene for our answers to Q9, here is a summary of the privacy protections outlined in the Consultation Paper, drawn from TDIF provisions, TDIF accreditation requirements, and the findings of the identity system PIA:

- *[avoiding] possible commercialisation of data and profiling of Users*
- *[avoiding] the development of a single national identifier or a national surveillance database*
- *[avoiding] gradual or incremental changes to the system that might result in an erosion of privacy over time*
- *adherence to the Australian Privacy Principles*
- *adherence to the Australian Government Agencies Privacy Code 2017 and the Notifiable Data Breaches scheme*
- *restrictions on the use of universal identifiers*
- *restrictions on the use of Biometric Information*
- *prohibit direct marketing and profiling*
- *ensuring the system remains voluntary, not mandatory*
- *prohibit the commercialisation of personal information*
- *prohibit the profiling of individuals*
- *restrictions on the creation and use of a single identifier for the whole system*

- *restrictions on the use and retention of Biometric Information*
- *requiring express consent from an individual or their representative to use the system to authenticate and pass Attributes to a service.*

9A) Should the proposed privacy and consumer protections listed be enshrined in primary legislation?

We would certainly like to see certain protections enshrined in legislation, including:

- an unambiguous prohibition on the creation and use of a national identifier or any single identifier for the whole system, and
- restraints on the use and retention of Biometric Information.

However I am not sure that the "commercialisation of personal information" or the "profiling of individuals" can or should be prohibited. Profiling at some level is central to many legitimate fraud controls; for example, banks routinely profile their customers' card based spending patterns in order to detect suspicious transactions. How could legislation differentiate these types of legitimate profiling from purportedly inappropriate profiling? Is there any sort of standard for undesirable profiling — or is it just the sort of thing where 'we know it when we see it'?

As for commercialisation of personal information, it would seem inappropriate for the legislation to dictate business models of Identity Providers. If Australia Post for instance was to find a business case for selling an "identity wallet" to end users, then that type of product sale might be seen to be commercialising personal information. Lockstep believes in the fundamental strength of the Privacy Act to regulate the appropriate use by businesses of personal information. This seems to me to be orthogonal to digital identity, so I would caution again the Digital Identity legislation enshrining its own view of privacy protection.

9B) Are additional protections required? If so, what?

See *4.3 Choice* and *6.3 Consistency of privacy protections* below.

4.3. Choice

The Consultation Paper states that "users *will* have the option to select from multiple identity providers to verify their identity" (emphasis added). A contestable marketplace of Identity Providers was one of the outcomes sought by the Murray Inquiry, and it was deemed essential by the TDIF PIA [3].

10A) Should the Legislation include rules around the extent of choice available to Users to verify their identity?

We do feel there needs to be mechanisms to ensure that a non-trivial choice of Identity Providers comes about and is maintained. The unfortunate experience of comparable digital identity markets and public-private initiatives (especially NSTIC and GOV.UK Verify) is that no commercially sustainable Identity Providers have emerged. If only a small number of IdPs emerge in Australia, and worse still, they are government services, then we face the prospect of a de facto national ID.

However, Lockstep is unsure what mechanisms there are to *guarantee* an ongoing choice.

10B) Should any types, or all types of relying parties be obliged to provide an alternative identity verification mechanism, and what exceptions should be available?

I don't understand this question. Why should offering "in-person or paper-based identification and verification" be obligated when Digital Identity is always optional? It is in fact Digital Identity that should be viewed as the "alternative".

For higher risk transactions, such as high value financial services and healthcare, the question that has gone unremarked is not about offering alternatives but rather the viability of digital identity. When will Relying Parties become comfortable accepting third party identification? In-person or paper-based identification isn't merely "traditional"; it is the *established* method for dealing with new users, and goes hand-in-hand with proven risk management mechanisms such as bilateral contracts and user agreements specific to the business. In high risk business, Relying Parties tend to undertake their own risk analyses (as of course they should) to guide how they identify and enrol their users. This almost always leads to higher risk service providers taking responsibility for enrolment and issuance of authenticators; that is, high risk Relying Parties tend to act as their own Identity Providers, in which a bilateral contract exists between service and user.

At this point, I suggest revisiting the fundamentals of Federated Identity and what it means for a Relying Party to drop its own user enrolment and switch to a third party IdP. The use of third party identity requires that the IdP underwrite or otherwise cover the risk of their identification going wrong or their authenticator technology failing, resulting in damage to the Relying Party. I have long argued that this liability shift has yet to be adequately codified by any large Federated Identity scheme. In [1] I wrote that despite the Laws of Identity showing how banks and governments act as Identity Providers,

> "few if any of these sorts of institutions have been convinced … to expand these roles, mainly because nobody has yet worked out how to allocate liability in multilateral brokered identity arrangements, without re-writing the contracts that currently govern how we buy, bank and access government and health services."

4.4. Restrictions on data profiling

11A) What types of profiling of behavioural information should be prohibited and allowed?

It is difficult to be specific about this in the current climate where there is so much innovation in behavioural biometrics, intention analysis, fraud analytics and so on. We need to be careful not to hamper the legitimate interests of businesses to seek out fraud signals for better risk management. While this is very much an important area of public policy and government direction, because unrestrained or opaque user profiling can definitely disadvantage consumers, I suggest that the legislation not prohibit any profiling across the board. Instead, let us look to existing privacy regulations to ensure businesses' collection of profiling data remain proportionate, reasonable, open and so on.

On a practical point, businesses are going to avail themselves of all sorts of fraud signals and profiling regardless of how the Digital Identity system works.

11B) Should a public register of Attributes be maintained?

Yes. Moreover, eventually there needs to be a standard taxonomy of Attributes so that when facts and figures about Subjects are provided in machine-readable form, all participants know precisely what they are dealing with.

11C) Should there be additional restrictions on access to Restricted Attributes?

I don't understand why there should be any restriction at all of this kind. I note that TDIF only defines "Restricted Attributes" indirectly, so it appears a little underdone in this area.

I can envisage many legitimate use cases where attributes such as Medicare Number or health identifiers could be usefully digitised, and, moreover, de-identified, and then packaged as verified credentials for a wide range of uses. The take-over of stolen Medicare Numbers is a particular longstanding problem which is overdue for a difgital solution. So I recommend a light touch in this area.

4.5 Biometrics

12A) Are there any other safeguards on Biometric information that should be included in the Legislation?

12B) Are there any that have been proposed above that should be modified or excluded, and if so, why?

No. I agree with the proposed biometrics protections and applaud the government's careful consideration of this difficult subject matter.

13A) Do you agree with the proposed approach for Biometric Information?

The overall approach seems strong, but there are a few logical inconsistencies, indicating that some more analysis or redrafting might be necessary. For instance, consider this passage:

> "It is proposed that the Legislation should limit biometric matching on the system to 'one to one' matching only. This means Biometric Information collected through the system could not be used by identity providers or credential service providers to match against databases or digital galleries containing more than one person's biometric template."

I find this somewhat contradictory. For one thing, there should be little or no biometric information residing in the Digital Identity system, because post enrolment, biometric images are deleted. I wonder what the scenarios are in which biometrics in the system could be used by identity providers?

For another thing, if the DTA is so uneasy about one-to-many matching that it would ban that mode, where does that leave other government processes which employ biometric deduplication (i.e. "Negative Identification")? One-to-many matching is routine in biometric drivers licence and passport issuance.

And consider this passage:

> "In the future, credential service providers may wish to offer Users the choice to use Biometric Information to authenticate to relying parties. Users could instruct their chosen credential service provider to encrypt and securely store their Biometric Information for authentication purposes."

I do not understand what is meant by "use Biometric Information to authenticate to relying parties". This seems to indicate an extra step undertaken by an RP using biometric information held by a Credential Service Provider for their (the RP's) own matching process. But what could that extra step be? If biometrics are only used in the Digital Identity system for one-to-one matching when establishing the identity in the first place, then the system surely has to be good enough to underpin subsequent use of the Identity without capturing and re-checking the Subject's biometrics. Furthermore, the proposition that any Biometric Information would be stored by a service provider (encrypted or otherwise) seems contrary to the overall direction that biometrics generally be matched on-device only and not retained.

13B) Will the limitations on Biometric Information overly constrain innovation or rule out legitimate future use cases?

Perhaps but so be it. "Innovation" cannot be allowed to proceed without reasonable constraints. It is entirely proper for the re-use of biometrics to be restrained. If government wants to avoid hampering innovation, then I suggest it loosen the centralised Digital System architecture, as discussed under *General comments* above.

4.6 Consent

14A) Should the Legislation specifically provide a mechanism requiring an individual's consent before the User transacts with a relying party?

No. Other privacy law covers this.

Digital Identity should be a tool available for Subjects and Relying Parties to better deal with each other. It does not seem appropriate for the Digital Identity system to intrude into how Subjects and Relying Parties interact.

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?

Yes. But one wonders why this would be necessary if the Digital identity system is always going to be optional. That is, no Relying Party would ever be allowed to force an individual to adopt the Digital Identity.

4.7 Age

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?

No.

If there was an age limit, then the problem would remain for certain RPs in certain circumstances to determine someone's age before granting them services. If for example there was a minimum age to get a Digital identity of 14 years, then the ATO would still be left to work out if someone is 16 in relation to TFN applications, and liquor stores would still need to work out if a customer is 18.

An unaddressed question is whether the Digital Identity legislation should specifically enable proof of age (or proof of birthdate).

4.8. Acting on behalf of another

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?

If person A (an "agent") is legally acting on behalf of person B (the Subject) in whatever capacity, then the identity question is this: How should the transactions carried out by A and the artifacts created by A be marked? Surely there needs to be a record of who the actor actually was and also who the Subject was.

While I am not a lawyer, it seems risky to me for a Digital Identity of the Subject B to be created and used by A such that it appeared that B was acting on their own. I would expect that legal conventions would dictate that the identity of agent A needs to be visible when A acts for B, and that there would be other layers of attribution to keep track of the fact.

4.9. Privacy Impact Assessments

Q17) Should the requirement for a PIA remain in TDIF accreditation requirements or should it be required in the Legislation or Operating Rules?

PIAs should be required in accreditation, one way or another. I don't feel strongly about whether they are called out in the Legislation or in the Operating Rules.

4.10 Human rights

Q18) 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?

No. I feel the Digital Identity system should be more or less silent on human rights, on the basis that this new system must surely exist within an overarching human rights framework. Anything on this score in the Digital Identity legislation would be redundant at best, and illogical at worst.

For example, one of the more interesting human rights questions is whether the transition from conventional analogue identification to digital identity is universally for the betterment of individuals, or whether the shift to digital might have unintended consequences for human rights. That question (obviously) cannot be answered by the architects of the Digital Identity system.

I do not for a moment suggest that the legislation and identity policy framework ignore human rights; the regime's designers must of course be well versed in human rights and anti-discrimination practices. But the *legislation* need not seek to expressly safeguard them.

4.11. Accessibility and anti-discrimination

I question the assumption that speed and ease of use are always for the betterment of individuals. Online fraudsters are generally notorious for exploiting the speed at which they can act once they subvert the system, and escape before being noticed. The assertion that "[by] facilitating fast and efficient access to a range of services, the system helps to minimise potential discriminatory effects based on age, race, disability, geographic isolation, gender or socio-economic status" is a non-sequitur.

19) Is the proposed approach to accessibility and usability practical and appropriate? Should any other considerations be taken into account?

If accredited participants are required to conform to the Australian Government Digital Service Standard and Web Content Accessibility Guidelines (WCAG) 2.0 Level AA (and if these overarching benchmarks are considered by relevant stakeholder groups as adequate, and they are enforced as a matter of course) then I see no need to add specifics to the Digital Identity regime. They might only get out of date or out of sync with accessibility and anti-discrimination norms as those norms evolve.

4.12. Penalties

20) What additional mechanisms, including penalties and redress mechanisms, should be included in the Legislation to prevent disclosure or misuse of personal or other information?

If the Legislation includes additional criminal offence and civil penalty mechanisms over and above the Privacy Act and the Criminal Code "including penalties for [not] protecting information used in the system" as the Consultation Paper suggests, then I do have no other suggestions to prevent disclosure or misuse of information.

4.13. Disclosure of personal information

21) Should the Legislation include provisions to enable the disclosure of information in specified circumstances? If so, what should those circumstances be?

There are plenty of models and precedents for exemptions to information protection obligations. I feel I have nothing to add in this area.

5.1. Independence

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?

There are established bodies which could be drawn on here, if we demystified the technical domain which needs overseeing.

If the exercise was purely about data quality (especially the accurate analogue-to-digital conversion of existing sources of truth) then the technical conformance challenge would be quite straightforward. The oversight body could be a conformance accreditation organisation such as NATA or JAS-ANZ. The management standard ISO 17025 (which forms the basis for the Common Criteria and Australia's software testing certification scheme) addresses *competence* and *independence* of certifiers, and even covers the interoperability of schemes internationally through Mutual Recognition Arrangements. With a slight course correction, from generic digital identity to more concrete data quality, the TDIF standards could be fitted to the ISO 17025 conformance oversight framework, and Australia could actually lead the way in interoperability of identity attributes globally.

5.2. Transparency

23) What type (or types) of information should be required to be publicly reported by the Oversight Authority, to increase transparency in the system?

The volume of identities provided and consumed is a key metric.

5.3. Accountability

24A) What is the appropriate period for review of the governance structure of the Oversight Authority?

24B) Should the Oversight Authority be subject to accountability requirements beyond those in the PGPA Act?

I have no well-formed opinion on these questions.

5.4. Functions and activities

25A) Are the roles and functions outlined above appropriate for the Oversight Authority?

No. I feel there are many potential conflicts of interest across that large set of activities.

As explained at section 5.4 of the consultation paper, accreditation involves "independent assessment of a potential Participant's ability to comply with the requirements of the TDIF before approving its accreditation". This process could be at odds with how accreditation normally works in industry, under NATA or JAS-ANZ administered standards. There, an independent certifier evaluates a candidate against technical standards, and the certifier's report is considered by an authority which weighs other factors such as health of the candidate's business. Separation of duties is needed between technical certifiers and ultimate accreditation, as well as ongoing complaints handling procedures.

I feel too many activities — some financial, some marketing or promotional, some operational, some customer-support related — have been grouped together under the oversight function. I suggest more work is needed to define and properly separate the following activities especially:

- **Service onboarding**
  - To "identify and brief government agencies and private sector entities with the potential to benefit from the system" sounds like a promotional activity which might conflict with accreditation and dispute resolution.
  - To "organise legal documents" must be clearly circumscribed. An oversight body might provide templates but to "organise" documents for an accredited system participant could be a step too far.
- **Service monitoring and incident response**. To "coordinate system-wide responses to critical incidents" will require careful demarcation of incident response responsibilities between participants and the exchange operator(s).
- **Investigations** needs to be separated from the other oversight roles of accreditation, dispute resolution, and fees and charging, so that one does not influence (nor be seen to influence) the other.

5.5. Advisory committees

26A) What other committees or advisory structures do you think may be needed?

No comment.

26B) Which other organisations or bodies could supply members of the Privacy Advisory Committee?

Lockstep has no particular favourites in this arena but there are many well established Civil Society organisations, and noted public intellectuals, who should be invited to participate in ongoing privacy advice.

5.6 Record Keeping

27) Should the record keeping requirements be outlined in the Legislation? If so, what should they be?

No comment.

6.1. Consistency across Australia

29) Is the proposed approach appropriately balanced to achieve the objectives of the system?

Yes. I strongly agree with the position in the Consultation Paper that the Legislation would not amend "other Commonwealth legislation by way of an all-encompassing override provision." We must beware unintended consequences, unexpected legal complexity and unbudgeted overheads incurred by efforts to change the effect of existing identification.

By and large, the Digital Identity regime should respect the sovereignty of existing jurisdictions and sectoral groups when it comes to determining their own identification protocols and risk management rules. Identification is usually a sub-set of risk management and as such, should always be defined locally. One of the unintended complexities of broad federated identity proposals (especially standardised Levels of Assurance) is they effectively seek to impose global identification protocols, thus pigeon-holing risk and up-ending local risk assessment.

Thus I contend that the Digital Identity system should expressly allow for the way existing credentials — such as driver licences, trade licences, professional qualifications, health and human services identifiers — are used currently. Instead of changing the meaning or status of existing credentials, it would be much more useful if the federal "identity" system provided uniform technical means to preserve the provenance and accuracy of those credentials. The Commonwealth has already made a great start in this vein with the DVS and FVS, which fundamentally make sources of truth — often state-based registries — available to Relying Parties, with convenience, uniformity, security and privacy. The DTA could work with various authorities to make more sources of truth available digitally, in the form of verifiable credentials, including for example Medicare numbers, Individual Health Identifiers (IHIs), Healthcare Provider Identifiers (HPI-Is), prescriber numbers, TFNs, ABNs, student numbers, training qualifications, work permits and security clearances.

6.2. Use of audit logs in judicial proceedings

30) Should the Legislation specify whether and how audit logs from the system can be used in court as evidence?

No.

6.3. Consistency of privacy protections

I find that the Consultation Paper's treatment of privacy tends to focus on formalities such as existing privacy laws and Privacy Impact Assessments. It should really go without saying that Digital Identity participants must comply with privacy regulations. And PIAs really are basic hygiene.

The paper and system design seem underdone with respect to the many ways in which digital identity systems can have unintended privacy consequences. There are structural features of the proposed architecture (such as the presumption of a central Identity Exchange and the way that all attribute presentation is mediated by the exchange) which are not intrinsically privacy positive. I would like to see more detail on how a central IdX would be prevented from surveilling all transactions running through it.

The legislation also embodies a critical assumption that there will be a choice of Identity Providers and Identity Exchanges. The second TDIF PIA states that "The entire model is built on multiple IdPs operating" [3]. Yet there is no privacy-protecting alternative or fallback should this assumption prove invalid.

Finally with respect to structural privacy protections, I note that "double blinding" (where IdPs don't know where identities are being presented, and RPs don't know which IdP issued a presented identity) is called out in the TDIF PIA as "the key privacy-by-design feature" [3]. Yet blinding is not mentioned in the Consultation Paper nor the Background Paper. If this feature is critical and if the PIA has been framed on the basis that double blinding is a fact, then I would expect it to be enshrined in the legislation.

Having said that, Lockstep actually has concerns for the novelty of double blinding because it removes the ability a Relying Party traditionally has to know where a credential has come from. To take a simple example, employers tend to ask where a candidate got their degree. More subtly, police forces often distinguish between different driver licensing bureaus because quality is known to vary from one to another. To remove the ability of RPs to know precisely which authority issued a presented credential could be a major disruption to how they manage risk.

Lockstep appreciates that the TDIF and the Digital Identity system promise to produce such a high-quality accredited array of providers that RPs will no longer need to know the IdPs. Nevertheless, the proposition that RPs can trust this new system instead of trusting their own assessment of a credential and its issuer has not been tested. Please do not underestimate the cost and time it will take for RPs to satisfy themselves that the new arrangements do not raise the RP's net risk.

31) Is the proposed approach appropriate to achieve a high degree of consistency of privacy protections?

I do not believe consistency is the main privacy problem; see above.

6.4. Administrative law and judicial proceedings

32) Should the Legislation specifically provide that additional administrative decisions relating to the system be subject to merits review?

No comment.

Conclusion

Thank you once again for this opportunity to comment on the Digital Identity Legislation. I would be pleased to discuss any of these matters in greater depth at any time. Very best wishes for the road ahead.

Sincerely,

Stephen Wilson
Managing Director

By e-mail.

References

[1]. Wilson, Stephen, "Identities Evolve: Why Federated Identity is Easier Said than Done" 2011. Available at SSRN: https://ssrn.com/abstract=2163241.

[2]. Wilson, Stephen, "A digital Yellow Card for securely recording vaccinations using Community PKI certificates", IEEE International Symposium on Technology and Society, 12-15th November 2020, Tempe Arizona (under review, accepted with changes).

[3]. Galexia, "Second Independent Privacy Impact Assessment (PIA) for the Trusted Digital Identity Framework (TDIF)", September 2018.

About Lockstep and the author

Lockstep (est. 2003) is an independent research and advisory group dedicated to digital identity, privacy and data protection. Lockstep Consulting has been engaged to provide digital identity advice and analysis for (among others) the U.S. National Strategy for Trusted Identities in Cyberspace (NSTIC), TDIF, the Australian Payment Council, Project Gatekeeper, the FIDO Alliance, the NSW Digital Driver Licence, Service NSW, Service Victoria, SA Health, the AGD's National Facial Biometric Matching Capability, Medicare Australia, the National Authentication Service for Health (NeHTA), the Open Identity Foundation, IBM's blockchain identity service, Evernym and the Sovrin Foundation.

Sister company Lockstep Technologies conducts breakthrough R&D on personal data protection and attributes management. We were contracted over 2016-19 by the U.S. Department of Homeland Security (DHS) through the Kantara Initiative to develop a mobile attributes wallet for first responders. Lockstep is the only Australian company to be awarded a DHS cybersecurity commercialisation contract.

I have long been involved in public policy for digital identity, with deep involvement with numerous trust frameworks, cross-sectoral federations and governance including:

- National Facial Biometric Matching Capability (undertook the first four PIAs)
- The AusIndustry-Internet Industry Association Authentication Hub (architect)
- New Zealand govt PKI (I developed the accreditation framework for offshore CAs)
- eASEAN (PKI subject matter expert in harmonising SE Asian e-signature laws)
- Hong Kong CA Recognition Office (technical lead in the new governance regime)
- The Biometrics Institute Trust Mark (researched and designed the certification)
- Australian banking sector *Trust Centre* (wrote the smartcard technology analysis)
- Webtrust for CAs program (Australian accounting industry representative)
- NATA IT testing Accreditation Advisory Council (expert member)
- NeHTA–NATA health software accreditation program (consulting member)
- sundry Gatekeeper PKI accreditations (I was technical lead at the first Gatekeeper accredited CA Certificates Australia Pty Ltd, Medicare Australia HeSA, the ATO's PKI data centre Gatekeeper impact assessment, and the National Authentication Service for Health).

I was a member of the Australian Law Reform Commission Developing Technology Advisory Sub-committee (2007-08), the National Electronic Authentication Council (1998-2001), the Federal Privacy Commissioner's PKI Reference Group (2000), the APEC eSecurity Task Group (1998-2001) and the Gatekeeper Policy Committee (2004-14).

More information is available at http://lockstep.com.au/about/identity.html and a broad selection of our research is collected at http://lockstep.com.au/library.html.