Digital Identity Legislation

Consultation Response

Christopher Betts
Dec 2020

Preamble

Recent events in 2020 have accelerated the rate at which Australians are conducing their everyday business online, and highlighted the importance of secure digital transactions as a national capability. This increasing digitisation has brought significant benefits, but also comes with increased and changing risks.

Digital Identity is fundamental to online security, however in general only the technical aspects of online authentication and authorisation are well managed. Identity verification remains problematic online, and the bulk of high-value online account creation is managed in-person.

This has two effects, only the first of which is commonly understood:

- Firstly, the cost in time and expense to ordinary citizens to do in-person identity checks is relatively high.
- Secondly, the transaction costs of performing these checks deters relying parties from doing identity checks unless there is a compelling legal or risk related reason, and many online transactions do not do such checks because the cost, user inconvenience, or privacy risk is too high.

This second effect represents a significant forgone opportunity, as it leads to an overall systemic lessoning of security both for citizens and organisations. For example credit card use generally only attempts to confirm control of the card, rather then the identity of the person using it – and credit card fraud runs annually to half a billion dollars. Similarly large numbers of 'low value' online transactions between schools, councils, sporting clubs etc. routinely ignore identity security, leading to regular data leaks and identity fraud (e.g. the use of Facebook for organising children's activities is widespread, with the accompanying data privacy and security issues).

The systemic benefits of replacing intermittent in-person identity checks with ongoing strong online identity are great, and the potential system-wide benefits of a secure, privacy enhancing digital identity that is ubiquitous, safe and easy to use are even greater.

In this context, the DTA's perseverance in creating usable standards for digital identity, reference implementations, and beginning the creation of an eco-system of providers and relying parties is to be commended. This is a difficult, long term task, however in many ways the DTA's efforts are in advance of those in comparable countries overseas.

Overview of Fundamental Issues

Digital Identity is a surprisingly subtle area, and it is important to understand that the fundamental issues are not technical in nature. In this context providing a legislative framework is very helpful, so long as the legislation does not make the mistake of assuming a particular technical approach.

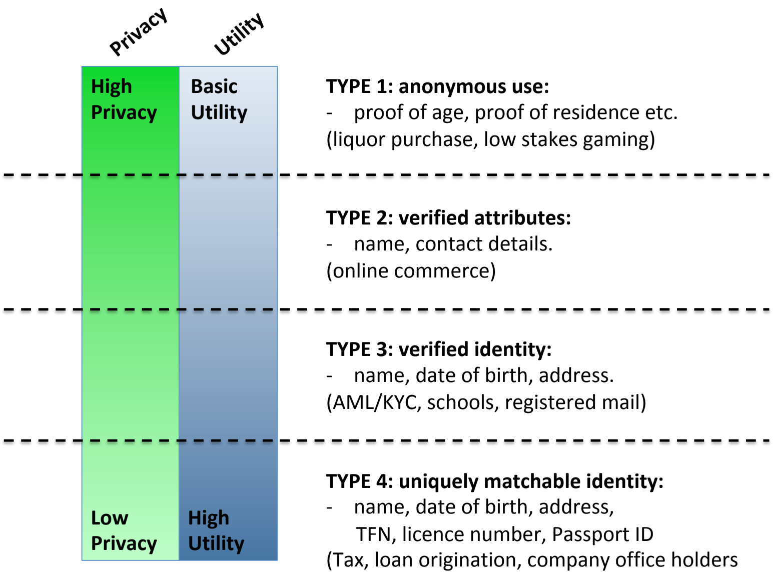
A quick review of some of the main challenges of digital identity in general, and of the DTA's TDIF approach in particular, will be useful.

Privacy and Utility

The first issue is that of Privacy. This is intrinsically difficult with digital identity, as the very purpose of digital identity is to prove who one is, which makes anonymity difficult. Frequently we attempt to enhance privacy by restricting data sharing between organisations – however this in turn runs into the problem that many digital identity use cases *require* that very sharing to be useful.

For example the widespread AML/KYC checks used in the financial sector are useless unless information about people making suspicious transactions can be shared with AUSTRAC in a way that allows matching. Thus digital identity mechanisms that inhibit data matching also undermine the very purpose for which the identity checks being made.

In fact, there is a clear tension between most 'high value' identity use cases and privacy, with the requirement to be able to match a user across different organisations being fundamental to the use of strong identity checks in the financial and government sectors. If a user cannot be matched across different financial transactions AML/KYC checks are pointless, as are the matching between financial organisations is required for loan origination credit checks , matching of office holders for corporate compliance purposes, tax reconciliation and so on.



TYPE 1: anonymous use:
- proof of age, proof of residence etc.

(liquor purchase, low stakes gaming)

TYPE 2: verified attributes:
- name, contact details.

(online commerce)

TYPE 3: verified identity:
- name, date of birth, address.

(AML/KYC, schools, registered mail)

TYPE 4: uniquely matchable identity:
- name, date of birth, address, TFN, licence number, Passport ID

(Tax, loan origination, company office holders

Privacy vs Utility

This is not to suggest that privacy is not important, but rather to point out that it must be managed in context, and can not be managed at a technical level. Currently the TDIF struggles with this contradiction, on the one hand attempting complex technical measures to preserve privacy (such as the TDIF 'identity exchange' mechanism), while on the other hand supporting functionality (such as document ID provision) which directly circumvent such measures.

In particular, the Identity Exchange attempts to prevent participating entities matching data at a technical level, by hiding relying parties from each other, and from identity providers. However since the information revealed in the course of transactions are generally attributes such as name, address, date of birth and so on, a reasonable degree of data matching will be possible for most purposes.

Further, allowing document identifiers to be passed through completely breaks any remaining technical privacy safe guards, as these document identifiers become a common key that can be used to match users between an identity provider and multiple relying parties. Government departments looking to do strong user matching for fraud and compliance purposes will use these document identifiers as a matter of course, at which point the entire purpose of the technical privacy safeguards built into the TDIF become moot.

Recommendation: *The TDIF should focus less on technical measures to enhance privacy, and more on legislative and contractual controls.*

Technological Implementation Barriers

A companion issue to funding Digital Identity is the cost of implementation. The easier it is to implement, the more likely it is that a digital identity ecosystem will form, and a 'virtuous feedback circle' will be created where citizens are able to safely and securely transact online, and companies can easily provide their services legally and appropriately.

An example lies in the common industry standards are used widely for integrating social media logins with websites. This has greatly reduced the number of login credentials users need to keep track of, as they can login with social media accounts such as Google, Facebook, Twitter and so on. Integrating these login mechanisms into a website is straightforward, and standard code libraries allow a software developer to integrate a range of login options into a website in half a day.

The TDIF approach is implicitly competing for mind share with the commercial sector, particularly the work being done in Open Banking and the Consumer Data Right (CDR). My belief based on successful overseas digital identity implementations (which are not common) is that both government and commerce need to co-operate for the 'ecology' to be successful.

There is simply too few government transactions for government identity to be successful on its own, and commercial imperatives mean that the private sector, with far greater volume, will simply not bear the costs of strong identity unless these costs can be minimised and spread across multiple parties.

The ideal analogue I believe is that of credit card payments. As commercial entities discovered the costs of maintaining credit card data internally, they turned to 'gateway providers' to manage credit card payments. Integrating these gateway providers into commercial websites is relatively cheap and simple, and the legal and compliance obligations of the 'relying parties' are quite low, as they keep no privacy or PCI/DSS information themselves. (The gateway providers on the other hand are more tightly regulated.)

A key feature here is that commercial providers can use the system without strong regulation, providing they follow basic rules. Similarly I believe we should enable 'low touch' digital identity use in order to be successful. Fintech startups are the quintessential example, where a need to do low cost AML/KYC checks has often been an impediment.

A final point is that the community sector is in terrible shape from a cyber-security point of view, and is generally underfunded. Anything we can do in legislation to drive the use of digital identity for non-profits and community groups should be encouraged.

Recommendation. *Legislation should be carefully written to encourage an eco-system involving government, commercial and community groups, and should not be limited to government usage alone.*

Identity Exchange and Legislative Opportunity

A key issue here is how the Identity Exchange will be used for Commercial and Community relying parties.

Currently, the Identity Exchange performs a number of functions:

1. As a technical convenience, it provides a single place to connect
2. It allows for complete control of the ecosystem, limiting who can participate to registered parties
3. It provides data separation, preventing anyone except the exchange operator from matching IDPs and users with relying parties – preventing commercial providers from data mining user activity information.
4. It enables a 'level playing field' amongst IDPs.

However by its nature this will act as a significant impediment to the development of an ecosystem:

1. It creates a single point of failure
2. It inhibits technical innovation by defining a single approved model for digital identity usage
3. It ads significant technical complexity and costs, which both inhibit takeup and raise the cost for all participants.
4. It makes some user workflows very difficult – e.g. users must be asked for consent multiple times, IDPs will be prevented from providing help desk assistance, and when users encounter errors they will not know whether to call the IDP, the relying party or the exchange.

However, as the DTA is considering legislation, we can see that the Identity Exchange is no longer necessary, as the requirements for control, for limiting the misuse of data, and for a level playing field are better dealt with in legislation. (If the government wishes to maintain it as a technical convenience for internal use it should of course feel free, but it is highly unlikely that commercial providers and relying parties will want to use it if given a choice.)

Recommendation: *Legislation should take over the problematic elements of the Identity Exchange, and use a legal and operating rules based approach to solve the issues the Identity Exchange was trying to solve at a technical level.*

Recommendations on Legislative Approach

In general, I have two recommendations for the legislation

Do Not assume a technical solution: *We should make sure the legislation does not assume a technical solution. E.g. difficulties with exchange are likely to make commercial identities separate eco-system; we want to keep door open for later adoption and technical innovation.*

Do not interfere with security best practice: *Similarly, we should make sure legislation does not interfere with best practice. E.g. requirements for a back door will weaken system security overall, and leave all Digital Identities vulnerable to a common attack vector.*

Feedback on Specific Consultation Questions

The DTA are to be commended again on their regular consultation with a wide variety of stakeholders.

The following is feedback on specific questions only.

1A - relevant matters

The legislative framework appears sensible.

1B – Additional Matters

Regarding further matters – commercial take up might be enhanced if we were able to clarify whether obligations such as AML/KYC were met by a particular TDIF digital identity level. As technology and security considerations are likely to change, it might be appropriate to grant the power of specifying that a particular TDIF verification level was appropriate for "AML/KYC Safe Harbour" to the DTA (possibly in consultation with AUSTRAC), to be determined as required from time to time.

2A – Coverage of Primary Legislation

Legislation should be careful to avoid mandating a technical approach. Specifically it would be a grave error if the Identity Exchange was to be written into legislation.

4 – Obligations on relying parties

We should leave open the possibility of a 'light touch' level of relying parties, where formal registration is not necessary - for example community groups and SMEs that use digital identity for registration as a gating mechanism to discourage spurious accounts, but do not maintain privacy information.

As discussed prior, we may be able to build an eco-system similar to PCI/DSS where 'final relying parties' out-source their digital identity checks to primary ID providers, but use the resulting information subject to privacy law.

5 – Definition of Digital Identity

There is a subtle assumption in the text that while a person may have multiple digital identities with different providers, they will only have a single identity with a single provider. However Identity Providers who operate at a high level of intrinsic privacy may not themselves be able to enforce this – and legislation should be careful not to impose such a requirement on providers. (Management of this issue should be delegated the level of Operating Rules.)

7 – Charging Framework

We need to recognise the systemic benefits that low-cost, low-friction digital identity brings to Australia's digital ecosystem. Currently driver's licences are used as a de-facto identity card within Australia, and the marginal cost of usage once the card has been obtained is close to zero – and yet this usage is widespread in clubs and pubs, for collecting mail, for gaming, proof of age and so on. In this case Digital Identity will have to compete against "free" physical identity checks.

However there are other usages where the cost and inconvenience of a '100 point check' (in all its variants) is a significant impediment to commerce, particularly for marginalised groups lacking good documentation.

We also need to recognise that most Australian Adults will need to perform a real-world identity check at some point of their interaction with the government, usually via the health system, tax systems, DHS or the education system. In almost all cases government acts an originator of identity information (although this may later be extended by commercial providers).

Further, there is the difficulty of how to encourage a market place of identity providers, and on what basis they can compete – particularly as the nature of the TDIF is that an identity check at a particular level is effectively commoditised (e.g. all 'level 2 plus' checks should be equivalent).

Finally, we need to understand that there is simply not enough usage of digital identity within government alone to create a viable digital identity ecosystem. Many citizens will only need to use digital identity to interact with government one or two times a year, and the volume is not enough for digital identity to be useful, as opposed to simply another impediment. As a proof point, the number of users who re-create a new 'MyGov' account every year is significant, as the service is used annually and users lose credentials or access to their mobile devices.

I suggest the following mechanism be adopted for Digital Identity within Australia, roughly following what I understand the Scandinavian system to be:

1: The establishment of a high quality digital identity be encouraged (and funded) by the government, as part of processes such as TFN issuance, DHS registration and myHealth records. This provides a common systemic good to Australia by making our online processes more secure and resilient.

2: There should be a market of providers, all of whom are paid an equivalent amount for a particular verification level, and who compete on usability to customers. Importantly, the government should be careful not to 'freeze out' commercial providers such as banks, post office and telcos by subsidising departments to perform these checks, or forcing the public to use a particular government service. The Swedish experience shows that the benefits to citizens will come through usage of Digital Identity across both government and commerce, with government providing the quality, and commerce providing the volume, of digital identity usage.

3: Usage of lower level IDs (say up to TDIF level 2 / "AML/KYC") be made free for commercial relying parties for an initial period of five years, in order to encourage adoption and usage. Identity Providers could be funded to supply this service on a cost recovery basis, or it could be made a requirement of registration (e.g. similarly to the obligation a service station has to provide air and water to vehicles in order to provide systemic safety benefits for all road users). After 5 years this could be reviewed and a small charge introduced, if appropriate.

4: A rate card should be provided for the use of higher level IDs (say TDIF 2 plus and greater), with IDPs being recompensed by relying parties. This should be a flat rate (e.g. there should not be a greater cost for the user's first ID check).

Notes on Charging Models

Overseas experience has shown that this is not a lucrative area, and Identity Providers need to be carefully encouraged. The UK market in particular has struggled with volume and the number and quality of providers.

One option would be a large number of identity providers. This would be possible if the legislative and compliance overhead were low, and the charging model straightforward. In this case a number of technology focuses providers (similar to credit card payment gateways) might appear. This seems unlikely however, as the volume is unlikely to support a large market.

Conversely, unless the government is careful, there will only be one identity provider, being the 'MyGovID' system or similar. This would lead to a government only identity ecosystem, as commercial providers and civil society would be cautious of using such a system, and the government provider would have little incentive to take on the risk and costs of providing a commercially focused system.

The DTA should consider carefully what sort of IDP market it wants to see – I would suggest a market with a small number of mature identity providers would be ideal. Further, I would suggest that the government does not want to be in the business of running these providers, in the same way as they are no longer in the business of running banks or credit agencies.

There are a number of organisations capable of running national IDPs, and as the Consumer Data Right (CDR) grows, many of these will also be building *de-facto* identity systems. The DTA should encourage these to be used also for government business, and aim to support a re-usable identity system that can be used for both government, social and commercial purposes.

8 – Liability

Liability should be managed similarly to credit checks – providing that an IDP has not made gross errors, it should be up to the relying party to select the level of risk they are comfortable with, and adopt the appropriate verification level for their checks.

In the event that an IDP has been grossly negligent they should be liable for fines and contractual losses.

Legislation would be an appropriate place to enable the creation of a number of offenses for gross misconduct, in a similar way to the obligations of a banking licence.

I note in passing that for any liability to be enforced, it would be necessary to 'lift the veil' on the Identity Exchange to reveal which Identity Provider provided the service to the relying party (see also sec 4.13 / Q21).

8D – User Support

As previously discussed, the Identity Exchange makes supporting users who are the victims of fraud problematic. Either the exchange provides secure privacy, in which case users cannot be assisted, or (as suggested in section 4.13) this is possible when desired, in which case the function of the Identity Exchange is superfluous.

21 – Disclosure of Personal Information

This is a good example of the intrinsic contradiction of using an Identity Exchange – in order to support a variety of use cases such as fraud, deceased estates, lost credentials or medical emergencies it may be necessary to 'lift the veil' and reveal the user's identity across IDP and multiple relying parties.

However the Identity Exchange as originally conceived prevents this, and hence will need to be specifically built in such a way as to allow this. In which case the value of the Identity Exchange becomes significantly limited to two primary functions:

1. It prevents an Identity Provider from correlating user information across different relying parties – however this could be managed by legislation
2. It provides a convenient 'single point of contact' for relying parties to connect to – however as we have seen with social media, a simple utility library can perform the same function at vastly lower cost.

Note on Encryption

There is a risk that a requirement for disclosure of information may inadvertently outlaw strong encryption. For example, the existing Australia Post Digital Identity solution relies on a two key solution that prevent either Australia Post or the citizen from unlocking the data in isolation – both parties must co-operate.

It is *very important* that legislation not prevent the use of strong security. Recent events have shown the importance of strong security, and how having a single 'gatekeeper' can easily lead to systemic compromise, particularly by nation state actors. Further, any attempt to create a 'backdoor' to Digital Identity will be seen as a sign of bad faith by the security and privacy community, and used as a rationale to resist what could otherwise be a significant improvement in online user security.

Conclusion

The DTA is to be commended for its widespread consultation, which has been a feature of its work since the beginning of the Digital Identity project.

Creating a strong digital identity that can be used across government, commercial and community use cases would be of great benefit, not just for individual citizens, but also for the general security of the nation. In the same way that fire regulation protect not just one person's house, but also their neighbours, strong digital identity can help improve the online safety of all Australians.