IEEE Society on Social Implications of Technology (SSIT) Australia response to

"Digital Identity Legislation Consultation Paper"

18 December 2020

Authors (in alphabetical order): [To be expanded]

Greg Adamson, Chief Risk and Security Officer, Medikey Australia.

Kayleen Manwaring, Senior Lecturer, School of Taxation & Business Law University of New South Wales, NSW Co-ordinator, SSIT Australia.

Kieran Tranter, Chair of Law, Technology and Future, Queensland University of Technology, School of Law, Chair SSIT Australia.

Stephen Wilson, Managing Director, Lockstep Consulting, Sydney.

Introduction

This submission has been prepared by members of the IEEE Society on Social Implications of Technology (SSIT) in Australia. IEEE is the world's largest technology professional association, with 420,000 members in 161 countries. Founded in 1972, SSIT is the unit within IEEE which addresses the relationship between technology and society. SSIT Australia was formed in 2005 and has members in all states. SSIT Australia members actively participate in the IEEE's Digital Inclusion, Identity, Trust and Agency program (DIITA),[1] which addresses many of the issues considered in the Consultation Paper.

SSIT Australia welcomes this opportunity to participate in the development of Australia's Digital Identity legislation. We agree with many of the considerations of the Consultation Paper, limiting our comments to areas in which we believe improvements may be made.

Offer to host workshop

As part of the Consultation process, SSIT Australia offers to host an expert workshop in 2021 focussed on issue of technology and society related to Digital Identity. We have the experience and network to draw together a senior expert group (12-15 people) for a one-day workshop. Previous workshops we have hosted for government and civil society consultations include:

- 2013: SSIT contribution to SAF05 Securing Australia's Future, ACOLA.
- 2016-2019: Workshops with Asian Development Bank and University of Melbourne on gender equity and social inclusion in renewable energy programs.
- 2018: Workshop (Brisbane) and submission to Australian Human Rights Commissioner's report on technology (later AI) and human rights
- 2018: Workshop on use of AI technologies in the homes of people with intellectual disabilities.

As an organisation within the technology community considering the social outcomes of technology use, a regular consideration is, "how will this use of technology affect vulnerable members of the community?" In particular, for vulnerable Users who may be preyed on by sophisticated attackers using social engineering, or treacherous or violent partners, friends or relatives, the introduction of

[1] https://standards.ieee.org/industry-connections/diita/index.html.

Digital Identity if not appropriately managed can open new means of victimisation. The expertise which we contribute primarily falls into this area.

General responses and specific question responses grouped by topic

Preliminary comments

The report makes an unstated assumption that because a User has a high level of confidence that the person or organisation with whom they are communicating is who they say they are, that the User can trust them. In relation to government agencies there may be a basis for this (the User knows the agency will be there tomorrow, and that there should be some process for redress), but in relation to private companies there is not. A fraudster may seek to defraud the User, even if they are who they claim to be.

Glossary: The definition of User as one who obtains a "digital service" is confusing. For example, if a User is unable to receive their pension, they may go hungry, not just lose digital services such as Netflix or Facebook. If a bank User is unable to make car payment, they may suffer physically. Digital Identity today can affect every aspect of a person's life, not just digital services.

Lessons from Identity systems

Q 5: The report includes a number of positive suggestions, including: avoiding a single identifier; restrictions on data profiling; restrictions on collection and use of biometric information; and express consent for User authentication. The additional point in 3.3.3 that a person may have multiple Digital Identities re-enforces these.

Q 6: The reference to "opportunities to support the operation of existing legislation" such as the AML/CTF Act 2006 (Cth) opens the door to the use of the Digital Identity for policing activities. Such use created immense uncertainty and suspicion in the introduction of My Health Record, and if this is included in the legislation, it could significantly undermine the inclusive goals of the program.

Q 9: While the report describes the extensive experience of the Digital Identity system within Federal Government, there is no reference to any lessons learned. Such a reflective consideration of past lessons would add to the credibility of the report and confidence in the ability of the Interim Oversight Authority to provide the protections promised in the report.

Q 24A: Given the rapid transformation of services and commerce which the Report hopes to enable, alongside the rapid evolution of technology and its use, the 5-yearly review of the Oversight Authority appears far too infrequent.

Digital Identity, vulnerability, exclusion

Q 4: The Consultation Paper states that the Digital Identity regulatory framework is "not intended to regulate the services provided by relying parties once an individual has verified their identity", although existing laws apply. Improved ID services may allow companies providing legal but detrimental services (particularly addictive services such as online gambling) to more accurately target individuals at the moment they are legally eligible to consume the service. The legislation should therefore consider the risk management question, "What could go wrong?"

Q 4: The framework may also be used by banks to reduce the extent of their obligation to give customers the benefit of the doubt in a case of fraud, as the customer ID may be considered proof that the customer did not exercise appropriate care in preventing the fraud. As banks currently absorb a large proportion of the cost of fraud, a reduction in fraud is a bank benefit, not a consumer benefit. A transfer of risk from bank to consumer would be a consumer detriment.

Q 4: The report is silent on how the responsibilities of Accredited Participants will be maintained if the company becomes insolvent or is subject to a takeover. For example, would the responsibilities past to the receiver? Would a takeover trigger cancellation or immediate review of Accreditation? This is an important consideration among small start-ups mentioned in section 6.3.3.

Q 10B: The suggestion that "smaller public and private sector services" would be allowed to mandate use of the Digital Identity appears to conflict with other principles in the Consultation Paper. In particular, if these smaller organisations are providing a critical service (food, shelter, childcare, education), then the Digital Identity system ceases to be voluntary. Several deaths in Jharkhand, India, have been attributed to failure to link ration cards to Aadhaar identity accounts.[2] While this may be far from the expected Australian experience, it should alert us to the principle that de facto compulsory identity systems can create risk for the vulnerable. In March 2020, approximately 2.5 million Australians were reported as having no internet connection, a significant barrier to accessing government services, online education and telehealth during the pandemic.[3] These people are among Australia's most vulnerable, and the economic downturn is likely to lower their financial capability of gaining internet access in the short to medium term.

Q 19: The report links anti-discrimination to "fast and efficient access" to services. However, the experience of Aadhaar cited above, and elsewhere shows that the more extensive the implementation of an identity system, the more severe the consequences for those who lack that identification.

Social and financial costs of the service

Q 8C: A significant gap in the Consultation Paper occurs in the proposed Recoverability mechanisms. This currently states that even with every Participant meeting their obligations, a Participant or User could still "suffer loss or damage". The proposals for supporting victims of cybercrime and identity theft in these circumstances appear weak, particularly limiting the Oversight Authority's functions to assisting Users "to identify the appropriate organisation to contact and support them through the process". Joining these together, this suggests that if no one is at fault, and the OA has no capacity to directly remedy the victim, the victim will be left to their own devices.

Even where there is identifiable Participant misbehaviour, given the complexity of the system it may take an extended period for the damage to be "made good". This contrasts to the obligation of banks following fraud in the cards system or direct debit (make good the customer, then address the fraudulent behaviour), which builds a high level of trust among customers.

Q 7: The report and legislation should not exaggerate benefits to consumers, particularly if there is a subsequent expectation that the consumer should pay at least partially for a benefit. For example, for a bank the program promises significant ongoing reduction in fraud and in AML compliance costs, while only providing a small convenience at the time of account opening for the User.

Human rights, privacy, and technology use

Q 10A: The framework relies on multiple Identity Providers to ensure choice in the system. However, this is undertaken in expectation of market behaviour. The framework should consider how to ensure choice if the government becomes the sole Identity Provider because other companies are

[2] https://www.business-standard.com/article/current-affairs/are-14-deaths-due-to-starvation-in-jharkhand-linked-to-aadhaar-glitches-118081100216_1.html

[3] https://www.smh.com.au/politics/federal/digital-divide-2-5-million-australians-isolated-with-no-internet-connection-20200327-p54egn.html

not interested in or withdraw from the market. Otherwise many of the concerns described in the paper may not be addressed, particularly the concern of one ID system implementing an “Australia Card” approach.

Q 18: It may have been a slip of the pen, but the suggestion that “human rights” only apply to “Australians” is surprising. An identity system in Australia which denied human rights to tourists, those on work visas, and other non-citizens would generally not be considered to meet the definition of complying with human rights. If a Digital Identity is only available to Australian citizens, then the framework should ensure that this doesn’t lead to breach of human rights for non-citizens.

Q 31: The report places priority on statute consistency, “Naturally, it is preferable for privacy provisions to apply as uniformly as possible.” An alternative view is that “it is preferable for all privacy provisions be raised to the highest standard of protection.” The assumption of “efficiency as a benefit” per se flowing through the report should be critically examined. From the point of view of technology, efficiency has no necessary relationship to societal benefit, eg the efficient production and distribution of cigarettes.

Q31 Section 6.3.2 sets out additional responsibilities for the Office of the Australian Information Commissioner (OAIC). The government has already faced public criticism for under-resourcing of the OAIC, within its current responsibilities. What sort of additional resourcing and funding will be provided to the OAIC in relation to its role in regulating the acts or practices of identity providers, identity exchanges and attribute service providers, including state and territory entities deemed by the new legislation as organisations under the Privacy Act?

Q 27: This section only addresses Commonwealth record keeping obligations. AFDA Express Version 2 (point 9) states, “In general, retention requirements indicate a minimum period for retention.” This approach is not aligned to APP Principle 11 regarding destruction of data. The Consultation Paper could usefully discuss the required modification of approach with the extension of Digital Identity to the private sector.