Submission on the Digital Identity Legislation Position Paper

Professor Kimberlee Weatherall[1]
Chief Investigator with the ARC Centre for Automated Decision-Making and Society
The University of Sydney Law School, The University of Sydney
19 July 2021

Overview

This submission responds to the Position Paper on the Digital Identity Legislation. It addresses the following points:

- The system should be framed to emphasise, and protect, core privacy principles including the right to anonymity and data minimisation. At present, the system normalises identity verification and provides no principles which will protect individuals wishing to interact anonymously. It is not sufficient to rely on APP2.
- The government needs to recognise that the creation of this system changes what is practical and changes incentives. By making it easier to verify identity, the government effectively encourages public and private sectors to request, or require, identity verification. Failure to provide counterbalancing principles requiring easy and convenient anonymity will, again, erode that capability and hence erode privacy, unnecessarily.
- The proposed accountability systems are inadequate: significant efforts are being made to *reduce* accountability of participants in the system for the harm it may cause, and there is no strong, well-resourced regulator established in the system. A strong, well-resourced regulator is necessary if individuals and their representatives are to be prevented from taking direct action to seek compensation for any harm that is suffered as a result of system failure.

The system should be framed to protect core privacy principles, including the right to anonymity and data minimisation.

1. In building systems for information verification, the government should be guided by the principle that interferences with fundamental human rights are necessary to achieve some other important public policy goal, and proportionate to achieving that goal.

2. Privacy is not just about the security of data and avoiding data breaches or identity theft. Two basic elements of the fundamental right to privacy are **anonymity** – the right not to be always identified as one goes about one's life – and **data minimisation** – the idea that an entity should only collect, store, and use the minimum amount of personal information necessary to achieve its goal. Privacy is also about people being able to exercise **choices** about to whom they reveal what information.

There is insufficient protection for anonymity

3. The Position Paper does not frame the system as one that protects anonymity.

4. First, it suggests that the legislation will 'describe the Digital Identity system in general terms as an information technology network allowing Users with a Digital Identity **to establish who they**

[1] The author can be contacted at kimberlee.weatherall@sydney.edu.au. Curriculum vitae and other information is available at https://www.sydney.edu.au/law/about/our-people/academic-staff/kimberlee-weatherall.html. This submission has been prepared with the assistance of Mr Jacky Zeng; views remain the author's own.

are online.' The system should be framed, not as a digital *identity* system but as a digital *credentials* system: one which enables people to establish that they have credentials which are necessary to access a given benefit or service, or engage in a given transaction.

1. Second, there appears to be no limit on what kinds of entities can become relying parties, or for what purpose, or the kinds of transactions or interactions for which relying parties can request that individuals provide a digital identity. The paper proposes neither a white list (these are the only kinds of interactions for which identity can be required) nor a blacklist (these are the kinds of interactions for which identity cannot be required). There is nothing in the Position Paper that seems to limit the potential set of participants to those which have traditionally and legitimately required information about identity.

2. On the contrary, in describing the legislation, the Position Paper states that the legislation will 'allow for a government body, company, trust, partnership or unincorporated association wishing to participate in the system as a relying party to apply to the Oversight Authority be onboarded to the system.'[2] The phrasing of the Position Paper points to an 'whole-of-economy' system. Whether intended or not, by framing the system as one where you can 'prove who you are', it suggests that it is *always* legitimate and appropriate to require identification.

3. Identity is not always required to be verified to achieve some legitimate goal of a private or public sector entity. For example, a person's entitlements to services or benefits delivered by public service entities do not always depend on identity, they may depend on other criteria: Australian citizenship; whether you live in NSW; whether you have a valid Medicare card.

4. Where the information necessary to be verified is not identity, but some other attribute, then tailoring systems to engage only in necessary and proportionate qualifications on the right to privacy would ensure that it is sufficient to verify that information, **without** passing on identity.[3]

5. More broadly, a person may wish to receive a quote on insurance without first identifying themselves, not least so that they will be able to shop around, engage in comparisons, and potentially investigate whether they are offered the same price on different occasions. This will become less possible if identity verification becomes ubiquitous.

6. Nor is this addressed by the *Privacy Act 1988* (Cth). The *Privacy Act* only limits the information which may be collected to that which is *reasonably necessary* to *one or more of the entity's functions*. Those functions could include marketing, personalisation, and customer profiling for marketing or personalisation of services, products, or contract/transaction terms.

7. While the Paper talks about Relying Parties' obligation (subject to exemptions) to provide alternative avenues for identity verification, it does not talk about alternative avenues for anonymous engagement. Despite the frequent claims to the 'voluntary' nature of the system, there is no obligation on public or private sector entities to provide equally convenient non-identified alternatives, or to limit their request for identity to circumstances where it is necessary to verify identity in order to provide some good, service, benefit, or information to an

[2] It is possible of course that an entity such as the Oversight Authority might accept only certain kinds of entities to join the system, or issue guidelines to that effect. However, any such expansion or contraction of participating parties

[3] A system is arguably tailored only to make necessary and proportionate invasions of privacy if it enables a person to *choose* to use the 'identity gateway' to verify other information, *provided that* there is an equally convenient alternative so that individuals could verify the necessary information without going through the identity gateway. But as noted further below, despite the frequent claims to the 'voluntary' nature of the system, there is no obligation on public or private sector entities to provide equally convenient non-identified alternatives, or to limit their request for identity to circumstances where it is necessary to verify identity in order to provide some good, service, benefit, or information to an individual.

individual. Nor is assessment of whether identity verification is necessary part of the stated criteria for allowing Relying Parties access to the TDIF.

It is not sufficient to rely on the APPs to affirm anonymity

8. *Australian Privacy Principle 2* states that Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter. Not all participants in the system will be bound by the APPs. APP2 is also qualified such that it does not apply if 'it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.' Finally, APP2 does not require that anonymous alternatives be equally accessible, obvious, or convenient for users. It is well known, by now, that considerable pressure can be exerted on individuals to share more information than they might prefer, through website and UX design and by making more private transactions far more inconvenient.[4] Unless anonymity obligations are built into the TDIF, it seems likely that incorporation of use of the TDIF will make it more likely that a Relying Party will see anonymous transactions as impracticable.

9. The Position Paper also fails to require data minimisation, suggesting there will be no limit (other than the *Australian Privacy Principles,* where they apply, and 'consent') to the attributes which a Relying Party can request or require.

The system claims to be voluntary without providing robust protection to ensure it is voluntary

10. The problems with consent as a model are well known and do not need to be repeated here. Relying Parties, it seems, will be able to request any attribute which is 'relevant' to any one of their functions (including marketing) and Users may, or may not be able to refuse consent and still transact with the Relying Party.

11. It appears that **consent** is the key mechanism for limiting the provision of identity information or attributes. The Position Paper relies heavily on a consent model to give effect to its stated objective of creating a system that is voluntary for individuals.

12. For all the reasons well-known in policy circles, and extensively canvassed in multiple government and public sector inquiries, consent is a poor mechanism for ensuring that any use of data is voluntary on the part of individuals:[5]

    a. Consent is frequently not genuine when presented in the form of an online tick box system that stands in the way of the consumer achieving some other goal (such as, say, booking tickets to an event);

    b. Consent is frequently not genuine when obtained online as a result of people agreeing to an extended written privacy policy which is unlikely to be read or understood;

    c. Consent is not genuine where a person is not offered a reasonable alternative. If providing a digital identity, or providing consent for certain information connected

[4] See the considerable literature on dark patterns: eg, Luguri, Jamie, and Lior Strahilevitz. "Shining a Light on Dark Patterns." University of Chicago Coase-Sandor Instittue for Law & Economics Research Paper. Rochester, NY: Social Science Research Network, August 1, 2019. https://doi.org/10.2139/ssrn.3431205; Paterson, Jeannie, and Elise Bant. "Should Australia Introduce a Prohibition on Unfair Trading? Responding to Exploitative Business Systems in Person and Online." *Journal of Consumer Policy*, 2020. https://doi.org/10.1007/s10603-020-09467-9.

[5] See the extensive discussion of this point by the ACCC in the *Digital Platforms Inquiry Final Report*, 2019.

to that identity is a condition of obtaining some good or service, providing formal consent is not an indication that the transaction is truly voluntary. I note that while the Position Paper proposes to require a relying party to provide 'an alternative channel to enable individuals to access its services', nothing in the text of the Position Paper requires that any such alternative channel be convenient or reasonable, meaning there is no disincentive to use website design to push people towards identity verification.[6] The Paper further states that exemptions may be granted for online-only services, and for small businesses.[7]

13. A consent model creates a significant imbalance: all the **costs** of maintaining privacy (and here, anonymity) are imposed on the **individual**. The private or public sector relying party is not required (or incentivized) to bear the costs of enabling individuals to exercise their privacy rights, by limiting the information sought (as discussed above), or by giving people alternatives to giving up their privacy, or enabling them straightforwardly and easily to make genuine and informed choices about which information to provide.

14. The Position Paper states (at 7.4.6) that users will be able to provide 'enduring consent'. It is submitted that 'enduring consent' should nevertheless have a maximum period for which it will operate; ie that renewal should be sought (say, once a year).

15. For the system is to be genuinely voluntary, there would need to be:

    a. An obligation on public and private sector entities to offer reasonable and convenient alternative ways of obtaining goods, services, benefits or information that do not require identification. There are obviously entities or transactions where identity verification is already required by law (such as to open a bank account); these could be specifically identified as exceptions to such a requirement.

    b. Strengthened requirements beyond just 'consent' to enable people to make informed choices. For example, the ACCC in the *Digital Platforms Inquiry* recommended the creation of simplified and consistent privacy policies, 'traffic light' style systems, the 'unbundling' of consent, and setting defaults against the sharing of information.

The Position Paper fails to address the impact the system will have on <u>incentives</u> to request identity

16. Currently, even aside from APP2, public and private sector providers have reasons to keep to a minimum the situations where identity verification is required, in order not to repel individuals/consumers from interacting with them (people will leave a site or store if required to go through too many steps).

17. The creation of a convenient, 'seamless' Digital Identity verification system changes that dynamic. It creates a strong temptation for both public and private sector Relying Parties to ask consumers to use this accessible and convenient system, which does not burden individuals/consumers with the need to go through multiple steps. Service providers have reason to prefer to use the Digital Identity system over past systems of simply requiring an email address. Relying Parties are therefore likely to require identity verification where it is not necessary, and/or to require more information than is strictly necessary, for a number of reasons, including:

[6] See sources cited above n 4.

[7] Query whether small businesses may be precisely the organisations that individuals might hesitate to provide with their Digital Identity, out of concerns over capacity.

a. Commercial pressures: data about people is valuable, and verified data about people more valuable than inferred data. Firms are likely to request identity more often than they need to, in order to link transactional and behavioural information to verified identity. There is a perception in the market that 'personalised is better', whether because personalised advertising is more valuable, or because it is seen as 'better' for consumers/individuals.

b. 'It might be useful': There is a current tendency, as frequently noted by various parts of government, to collect more information rather than less, on the basis that 'it might be useful' at some point for data analytics, and on the basis that collecting it involves only limited costs in a situation of widespread and low-cost availability of data storage.

c. Simplistic problem solution: Identity verification is often proposed as a solution to problems unrelated to a need for identity, and without regard for broader potential consequences of requiring people to identify themselves. For example, it is common to see calls for social media platforms to require and publish the identity of users of the platform, with the idea that this will reduce undesirable behaviour on such platforms (such as trolling and harassment). Identity has not been shown to solve these problems. It also creates its own significant risks for people with legitimate reasons to wish to conceal their identity, such as victims of stalking, harassment, or domestic violence, or people who simply wish to interact with the world without people being able to link them to their activities.[8]

18. I noted earlier that there is no stated limit in the Position Paper on what attributes can be linked to the Digital Identity system, or what kind of entities could become attribute service providers. Degrees or qualifications are mentioned as a possible information attribute that could be provided by an attribute service provider, but it is unclear what other attributes might be added. This has two likely effects:

a. It increases the range of entities likely to become Relying Parties (ie parties who require information about some additional attribute), who will therefore be more likely to collect and use information about identity.

b. It increases the interference with the data minimisation: it enables relying parties to request those attributes that have been linked into the Digital Identity system, even where not strictly necessary to provide goods, services, benefits, or information to an individual.

19. For these reasons, the government should consider rules, or at the very least principles, which require Relying Parties to minimise the occasions on which identity verification will be sought to those where it is necessary; to limit attributes requested, and to make anonymous options equally prominent and convenient as more privacy-invasive practices.

Enforcement: The Position Paper outlines a system with insufficient accountability mechanisms.

20. The accountability mechanisms outlined in the Position Paper are insufficient.

[8] Other legitimate reasons for keeping identity secret could be, for example, to avoid employer concerns about employer reputation based on employees' non-work lives. People may wish to conceal their gender or their parental status to avoid harassment or discrimination. Too often public and private sector entities fail to take into account the full range of legitimate reasons why people may not wish to reveal their identity, on the (false) basis of, 'if you have nothing to hide you have nothing to fear'.

21. As the Position Paper recognises, accountability is an important part of ensuring trust in the system. Assessing accountability means asking four key questions: *who* is accountable, *to whom*, *for what* and *how*? In looking for accountability, we should be looking to see whether government entities are accountable for their exercises of power, and whether parties (in particular individuals) harmed by the failures of actors within the system have mechanisms for seeking redress.

22. The Position Paper persists in a model well-known in Australia in privacy-related areas of policy, where:

    a. The government entity acting in a government capacity – here the Oversight Authority – is answerable to the usual political processes, and as it affects corporate participants can have its decisions overturned. But it is not liable for harm caused to individuals (via lax oversight, monitoring or accreditation decisions) or corporate participants;

    b. Commercial participants are accountable to the Office of the Australian Privacy Commissioner (OAIC) (which 'monitors' compliance with privacy) and OA (which can audit them, and potentially remove them from the system) and to each other (if breach causes harm to another participant, but only if that other participant can prove that they breached the rules *and* failed to act in good faith. Commercial participants' only accountability to individuals appears to be indirect – to assist with recovery from identity theft (if told to do so by the OA) or address privacy concerns (if told to do so by the OAIC). The Position Paper does not make clear whether there are any breaches which would lead to immediate suspension of participation in the system.

23. There is very little accountability for **relying parties** under the system. This may be because the government is relying on general privacy law to ensure accountability. Both current Australian Privacy law, and regulatory systems, are known to be insufficient (as recognised by the current review), and unless and until it is strengthened, it cannot be relied on to provide discipline that would justify people trusting the TDIF.

24. **No one** appears to be directly accountable to individuals harmed via the TDIF or organisations representing their interests. All the burden of enforcement and monitoring is placed on the (chronically underfunded and underpowered) OAIC, and an OA which depends on secondment of department staff for all its resources (and will hence no doubt be subject to the usual efficiency dividends and public sector diminution).

25. There is no mention in the Position Paper of **compensation** for individuals harmed through the system. There is a vague mention of insurance, but no clarity regarding whether parties will be required to be insured sufficient to compensate individuals harmed through data breach or identity theft.

26. Over-extensive requests for digital identity verification and/or attributes will be difficult to subject to oversight under the proposed system. Oversight focuses on the moment of **joining the system** with consideration of (legitimate) questions whether an entity meets the necessary technical and competence standards, as well as broader national security and system risks issues. For relying parties, it also appears to ask whether the relying party is a 'fit and proper person'. This does not appear to ask whether the purposes for which identity verification is sought are legitimate, or necessary.

27. The Position Paper is also very unclear in relation to accountability for automated decision-making. On the one hand, the Paper suggests that there will only be liability for breach where a

party fails to act in 'good faith'. On the other, the Paper also suggests that parties might use automated systems to take actions. It is very unclear what the government's position is regarding whether (or when) failure of an automated system could be considered to involve breach that is not 'in good faith'. The Position Paper contains only the highly unsatisfactory sentence, 'Participants operating in the system should ensure their use and reliance on any automated decision-making process is acceptable to them in light of any laws they may be governed by.'

Biometrics

28. The Position Paper states that the legislation will 'allow for rules to specify permitted and/or prohibited biometric modalities … that can be used'. It is unclear who would make or propose such rules, and what consultation process would be involved. Biometric information is particularly sensitive and has a history of differential accuracies in relation to different groups across society (gender, race). It has more than once been suggested that there is a need for a specialist oversight body to address the use and impact of biometric identifiers, and to make rules for their appropriate use. The *absence* of such a specialist entity puts Australian's privacy at considerable risk. This is another context in which this is obvious. It is not at all clear that an Oversight Authority whose primary functions relate to the operation of the TDIF is the right body to making rules regarding biometrics.