VeroGuard Systems

18 December 2020

Re: Proposed Digital Identity Legislation

Dear Sir/Madam,

We welcome the opportunity to provide a submission to the Consultation process into the review of the Australian Digital Identity Legislation.

We preface our submission with a statement about digital identity that, we believe, must underpin the Australian Digital Identity Legislation.

> ***Critical to protecting information technology and data is the accurate and reliable verification of the identity of a user that needs to access any network services and information. In the absence of proper identity verification, all other security measures are of little effect or use when a criminal incursion is disguised as coming from a trusted source.***

Cybersecurity Ventures expects global cybercrime costs to grow by 15% per year over the next 5 years, reaching US$10.5 trillion annually by 2025, up from US$3 trillion in 2015. This represents the greatest transfer of economic wealth in history.[1] Australia is neither immune, nor experiencing anything different, from this global experience.

The growth in cybercrime is largely driven by the proliferation of people, end points and applications moving online, bringing with them substantial associated increases in the volumes of personal and identifying data being collected and exposed. Crime rates are being compounded by the fact that existing and planned identity solutions are simply inadequate to meet the challenges of these changes, with compromised identity credentials associated with over 80% of all breaches.

Insisting on uncompromising security and privacy features for Australia's Digital Identity system is critical for our economic prosperity.

We would welcome any questions or clarification requests about our submission.

Yours Faithfully,

H. Daniel Elbaum
Chairman and Co-CEO
VeroGuard Systems Pty Ltd

Nicholas Nuske
Director and Co-CEO

[1] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

VeroGuard Systems

Consultation Questions :

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

These matters are relevant matters that should be addressed by the Legislation.

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

There is an important additional matter that should be considered for inclusion in the Legislation. The Legislation should mandate security standards to be adopterd by all participants.

The reality of cybercrime is that detection and remediation is almost always too little and too late. In the same way that an out of control pandemic overwhelms resources and contributes to the problem, the current cybercrime response approach of risk accepting weaknesses in cyber security will, in our view, end up being catastrophic to economies and overwhelming cyber security detection and remediation resources.

Cyber security and cybercrime are moving at a rate that is faster than legislation or governing groups can respond to. There is already a significant disconnection between current frameworks, responsible security standards and commercial models. As securing digital identity cannot be left to chance or delegated, the Governments' clear responsibility should be to address this risk weakness through the Legislation by extending protections and governance to cover mandatory security standards. Digital Identity must be seen as a vital part of Australian infrastructure that both enables and protects our economy. Uncompromising security standards that are consistent with established and proven security methods and the opportunity to change and adapt them as conditions evolve must be an integral and mandatory part of the Legislation. It is not sufficient to simply ask that participants use 'best efforts' to address the issue.

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

In the same way that key privacy and security provisions are proposed to be taken out of the TDIF and included in the Legislation, mandatory security standards to be adoped by participants should also be included into the Legislation.

From our review of the Consultation paper and the history of the framework, it appears that the secruity standards are not proposed to be inlcuded in the Legislation but, perhaps, dealt with in the Operating Rules or TDIF. In our experience, it is simply not possible to maintain privacy, data integrity and digital security without clear mandated security standards. For example, the banks established secure authentication and communication rules (AS2805 ISO8583) and implemented infrastructure to meet those rules (for example the ATM/global financial networks). Banking governance globally in countries is legislated for chain of custody. Our digital identities and the ability to make them secure and protected must be enshrined in the Leglislation and not left for framework interpretations.

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

Defining the roles and operating responsibilities of the participants.

Providing assurance about usability and interoperability of processes and data. With always end to end chain of custody.

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

Defining requirements for the proper operation of the federated identity system.

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

No.

The integrity and trust in the system governed by the Legislation must be underpinned by transparency and clear, simple, information about what the system is, how it works and who is participating. Despite the need for transparency, ultimately business and citizens will expect Government to effectively assess and manage the underlying infrastructure that enables and protects us online. It is likely that most users may never rely on or reference any register. A poorly explained process and the requirement for separate, but dependant, verification registers is also likely to be confusing. The Digital Identity Participant Register is essential: however, the communication strategy about participants or users must be independent and simple. Such a system must ensure the privacy and control over the use of the digital ID remains in the hands of the citizen/end user always.

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

None suggested.

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?

The success of digital identity acceptance and use on a broad basis is heavily dependant on the Digital Identity being trusted by all parties. Therefore, the concept, language and definition of 'Digital Identity' and the underlying concepts compliance to standards and law are paramount to the success of the anticipated efficiency and security benefits of a full Digital Identity deployment. In particular:

- A Digital Identity should ONLY be relied on if it is tethered to a verified person. Therefore "…only one person," should be referred to as "…only one 'verified' person,".
- A user should also have, and be allowed to have, only one Digital Identity with each or any one identity provider.
- A Digital Identity allows a relying party to verify a user, but it is the relying party's own rules and permissions through their access management that allows a user to access or interact with the relying party's services.
- A fundamental principal of a secure Digital Identity system is to verify with assurance that the user is who they say they are without transmitting identifying data (such as attributes and biometric data). Attributes must only be used to create the ID and then never be available to anyone except the owner of the attribute. A system that allows or in the worst case relies on such electronic transmission has a high probability of misuse and catastrophic breaches. A Digital Identity should verify a user or their attributes and eliminate any chance to retain, retrieve or reproduce the information for the recipient.
- The concept of inclusive and accessable Digital Identity should be included.
- The concept of security and high assurance should be included. The success of the system and relying process demands trust in and the reliability of the underlying end to end security in the supporting platforms. In centralised systems, such as the Estonian Digital Identity, the security can be adjusted constantly to reflect the rapid and changing needs of cyber security (for example, the unreliability and limited ability to secure biometrics, particularly on smartphones, constantly needs new techniques or technology layers as each new biometric method is compromised by criminals). In a federated framework, this ability to constantly adjust will not be available due to the complexity and dependance of multiple parties. Instead, the Government will need to be define security and

privacy standards so that providers are obliged to adjust to maintain security integrity. To achieve this, exactly what security means, needs to be clear in the Legislation, otherwise it is certain that the framework will be constantly compromised as frameworks adjust to changing threats.

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?

The Legislation should not conflict with existing privacy or information legislation. It must complement and facilitate existing privacy or information legislation's secure use with appropriate permissions, protections and penalties. It is critical to adjust existing legislation, if required, to support the digital environment, rather than have multiple and, potentially, conflicting definitions.

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

It is proposed that users not be charged, but relying parties be charged, a single charge for the use of Digital Identity. In our view, this model presents insurmountable challenges.

A transaction based model is impossible to budget for as the volumes of requests are unpredictable. Historically, users have typically taken on the cost of other forms of identity, such as paying for birth certificates, passports, licences, etc. Whilst relying parties should definately get the benefit of efficiencies, most relying parties will already have established a customer online identity and will, in most cases, still need to maintain access management services.

If the charging model is predefined to the relying party, it is unlikely that the right platforms or a competitive market will develop or be maintained and the entire burden, as it is currently, will continue to fall on the Federal Government.

A user pays model would rationalise use and drive a better cost/value acceptance of the program.

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

Losses could be significant under failures of a Digital Identity platform. It may often be difficult under a federated model to assess where the failure occurred, including if the original design and compliance standards were insufficient. It may well be an inherent flaw of the framework itself to leads to the largest losses.

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

Participants should only be held liable for loss or damage suffered by a Participant or User under the liability framework in circumstances where it can be demonstrated that the loss or damage is directly caused by a Participant's failure to comply with the system's rules and requirements and that failure resulted in a breach of User data or a misrepresentation of a User or their data.

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?

Economic loss or damage claims could be made specific to the incident.

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

Level 1 support should be centralised. The experience of dealing with the NBN rollout and the multiple contact points is a good example of poor stakeholder and user experience. When dealing with identity, this needs to be very carefully considered.

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

Yes.

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

Inclusion and accessability.

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

Transition periods are required to allow for multiple forms of verification to be used to ensure that citizens (particularly disadvantaged people) can continue to access services. For example a requirement to have a certain type of smartphone or particular physical characteristics that are not biased against by biometric software are clearly not only discriminatory but impracticle to implement. The framework and consultation document seems to be avoiding existing mechanisms that could be utilised to deliver better more secure outcomes that are already well established from a technology, security and user experience perspective, such as Interbanking systems. These existing systems would not only accelerate adoption but remove the risks inherent with biometric authentication.

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?

A number of characteristics of the proposed system make it impracticle if not impossible to have relying parties not offer alternative mechanisms. For example the requirement to use certain types of smartphone, concerns over biometrics, the risks of attributes being breached, the reliance on opt in model, an unpredictable charging model etc.

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

All types of profiling of behavioural information must be prohibited.

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

No.

Attributes should be User controlled with the User's chosen provider. The current proposal of allowing certain Attributes to be transferred between providers with User permission is likely to result in significant misunderstandings with unanticipated consequences for the User and inappropriate use of Attributes.

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

All Attributes should be User controlled and used only once.

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

The use of Biometrics at any point of authentication introduces substantial privacy and security risks. Avoiding Biometrics altogether would be a substantially better approach.

Whilst the paper details mitigating suggestions to reduce the privacy and security risks, the exploitation of any biometric system can be catastrophic for Users. Once compromised, a User's biometric cannot be simply replaced in the manner of a password or PIN. In controlled, closed loop, systems, such as passport control at borders, this issue can effectively be managed. But, in open networks relying on variable hardware and software on User devices, the risks are substantial and cannot be effectively managed.

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

There are better, more secure, approaches that do not require Biometric data to be used. The National Security Agency of the USA recommends for secure authentication, PIN's (something a user only knows) with physical security mechanisms (something the user has and that is also built to be tamper proof). Banks have successfully used this framework for over 30 years to transfer trillions of dollars each day through their networks. This architectue is now available for online identity through the VeroGuard Platform and eliminates the need and substantial risks of biometrics.

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

No.

Biometric systems for digital identity, particularly when using consumer interfaces for authentication, carry significant risks. the exploitation of any biometric system can be catastrophic for Users. Once compromised, a User's biometric cannot be simply replaced in the manner of a password or PIN. In controlled, closed loop, systems, such as passport control at borders, this issue can effectively be managed. But, in open networks relying on variable hardware and software on User devices, the risks are substantial and cannot be effectively managed.

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

The limitations, risks and privacy issues associated with Biometrics will, for the foreseeable future, both limit future use cases and provide unacceptable risks for Digital Identity. Biometrics have a place in recognising a User, but no role in verifying a User outside of a controlled environment.[2]

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

Yes.

Substantial risks exist in this model, with Attributes being forwarded each time a User transacts with a relying party, rather than just verifying the User. A User must be informed of and consent to those risks each time. Users should have complete control over any Attributes or data provided to a relying party.

[2] https://www.csoonline.com/article/3330695/6-reasons-biometrics-are-bad-authenticators-and-1-acceptable-use.html

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.

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?

Anyone should be able to have a Digital Identity, but, under a certain age, only with parent/guardian's consent.

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?

Nominees should not have the opportunity to represent themselves as another person, but should be able to act as a delegate for a person with the correct permissions as per any other form of identity based transaction.

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

All aspects of privacy and security should be considered for inclusion in the Legislation.

18) 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?

Digital Identity should be a right for all Australian's and recognise disability, socio-economic factors, remote and regional considerations, race, domestic violence and age as high priorities relating to access and human rights.

19) Is the proposed approach to accessibility and usability practical and appropriate?

Yes.

It may be that not every disability can be catered for initially and the plan can cater for continual improvement.

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?

The Legislation must take into account the multitude of parties to a potential breach to ensure that relevant parties are held accountable. For example, more Attributes than were authorised are passed to a relying party, who has stored and not yet deleted the Attributes in a third party cloud provider who received security certification but was breached by an identity compromise of their domain credentials. Who is liable for the loss of the data and consequential damages?

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

Exceptions will cause security exposures and should be avoided whenever possible.

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?

An Oversight Authority should be able to provide effective and independent governance of Digital Identity. Recognising the significant exposures to privacy, security, human rights and economic prosperity, the Overrsight Authority should also have available a wide range of experience to execute it's role effectively. This means that a new body should be established and include an advisory group across the key aspects of Digital Identity.

22B) What is the optimal structure of a new body?

A new Corporations Act company.

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

Added to the list could be the number of unique Attributes transferred and the average number of Attributes transferred per User.

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

Due to the fast pace change with digital transformation and cyber risks, the first review should take place after two years and then every three years theraafter.

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

Platform security accountability should be strengthened beyond PGPA - for example, the PSPF**.**

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

Mostly, although the mandate seems to be limited to an administrative function. Even as an administrative function, the Oversight Authpority would need support in many specialised areas and have the ability to draw on expertise from other specialised Government agencies (ACSC, Digital Health, OAIC, etc)

25B) Are there any other functions that should be undertaken by an Oversight Authority? If so, what?

The Oversight Authority seems to be taking on an administration role rather than an effective steering and goverance role. Advisory and governance groups are vital for the success of the system. These may or may not be included in the Oversight Authority, but are vital for success of the system.

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

The Oversight Authority seems to be taking on an administration role rather than an effective steering and goverance role. Original issues with electronic health and electronic health records inlcuded the lack of industry participation and expertise associated with the steering and governance of electronic health. This was resolved when NEHTA became the Australian Digital Health Agency and greater stakeholder and relevant expertise was incorporated to the board, staff and committees. This real world practical approach is adopted for Digital Identity in other countries such as Canada, where a board and committees are representative of all stakeholders, particularly on the TDIF advisory committee. Key aspects to the success

of the system include privacy, identity security, functionality, user experience and should be included in one or more rlevant committees.

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

It would be advisable to have representation from relying parties and other providers involved in the system.

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

Yes. They should reflect other record keeping legislation and inlcude express requirements to delete certain information such as Biometric data.

28) What best practice models should be considered for the protection and use of the trust mark?

Having a trust mark is likely to provide a platform for fraud and scams despite having penalties for misuse. For example a criminal would be able to use the trust mark to gain trust of a victim irrelevant of potential penalties. A better approach would be to have a non-repudable system in place that is trustworthy and not subject to credential compromises.

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

Yes. It will, however, need to go through a review process after operating to determine practical examples of conflict when operating.

30) Should the Legislation specify whether and how audit logs from the system can be used in court as evidence? If so, what should the Legislation say?

As the Digital Identity system and process has varying levels of proofing, identity security and assurance, audit logs should be specifically excluded from evidence. Audit logs could only be used if non-repudiable Digital Identity is used to guarantee chain of custody.

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

Yes. It should be noted, however, that privacy is at risk in this system as part of it's design.

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

Yes.

About VeroGuard Systems

VeroGuard Systems Pty Limited is a cyber security company with a head office in Melbourne, Australia and a significant manufacturing facility in Edinburgh, South Australia. The VeroGuard platform was initially developed and patented by Daniel Elbaum in 2003. The platform successfully brought the security protocols for interbank communications to the internet (anywhere globally) for the first time and, by 2011, was certified in trials with banks across three Asia Pacific countries. In 2016, recognising the significant opportunity to solve the world's most pressing issue for online security (identity credential compromise),

Elbaum successfully adapted the platform as a full identity layer for the internet to provide the first and only non-repudiable Digital Identity for guaranteed ID online.