IBM **Digital Identity**

Submission to the DTA

December 2020

Proposed Digital Identity Legislation

Submission to the DTA

18 December 2020

IBM Response

IBM is pleased to provide input into the DTA consultation process on the proposed legislation intended to support and strengthen an expanded digital identity system in Australia.

IBM has a proud history within the Cyber Security domain, with the first acquisition of capabilities being a company called DASCOM in 2000, a company founded by Australians. This acquisition enabled IBM to deliver widespread ecosystem solutions that are still in use by major clients throughout Australia. IBM has since employed many Australians through its IBM Australia Development Laboratory on the Gold Coast, where today over 80 people work on security software exported to the world.

As a Cyber Security company, IBM recognises that secure digital identity is a critical element of any enterprise security program. We support the implementation of an expanded digital identity system that can be a whole-of-economy solution connecting federal, state and territory services, as well as private sector services. We believe that it has the potential to offer a greater choice for citizens, a more streamlined service, and a reduction in complexity. IBM looks forward to playing a key role in engaging our clients and working with the government through this process.

Delivering digital trust in an ecosystem requires the management of the cyber security threats, in support of providing authentication and single sign-on capabilities. IBM recommends that the digital ecosystem consider cyber threats and risk as part of the ecosystem framework. As such, the following high-level themes may be considered:

- Registered authentication methods and use is one element of making risk-based decisions for access. The addition of other context in a decision framework would enable a stronger risk-based approach. For example, higher value or higher assurance levels of identity could have minimum requirements required by the providing party in terms of security assurance. The intent is not to be prescriptive, but to assist in provider's use of the platform being appropriate to the services offered and how it is protected.
- Delivering digital trust requires that service providers are able to manage threats. This system will be a target for adversaries, and there exists strong cyber security solutions for managing these threats, enabling the ecosystem to detect and respond in support of delivering digital trust to participants.

In support of these themes, IBM responds to a select number of questions as part of this consultation.

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

IBM believes that the relying parties should be required to share information about their practices as it relates to fraud or cyber detective or protective capability. The objective of doing this is for the government to gain an insight into the risk management governance that is being provided across the ecosystem. Since this is an interconnected system, this information will help to inform the government of relative capacity to detect identity-oriented fraud across the ecosystem. This would also help to inform government of ways that the ecosystem could be protected into the future.

IBM notes that while appropriate legislation is essential for a platform of this significance to protect consumers effectively, inherent trust in the platform is also an essential consideration for the Australian Government. We acknowledge that balancing trust through legislation and controls against the risk of stifling innovation from service providers is a key consideration. However, as this proposed platform is facilitated by the Government, consumers will inherently assume a level of trust and oversight has been performed as part of onboarding of providers for services offered. Having a clear view on what risk-based obligations the Government deems as needed for services, assurance levels or transaction values should have due consideration as the framework is developed.

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

A charging mechanism should take into consideration the benefits being delivered to the relying party. In many industries, a company's business relationship with its clients is underpinned by the trust placed upon them to safeguard their portfolio (including identity). Organisations that place consumer trust high on their list of priorities have raised concerns about the ability to detect threats across integrated ecosystems (such as consumer data rights).

In this case, integration of a new identity provider may introduce new risk vectors for those organisations, and any charging frameworks should reflect that. For other organisations, there are significant cost savings gained by eliminating the need to manage an identity lifecycle. Any charging mechanism should therefore be flexible to consider the range of benefits gained from participation in the ecosystem. The eventual extension to a whole of economy system needs to build in a charging mechanism that is fair and reasonable for small to medium businesses, and potentially not for profits.

In addition, with a goal of providing the safest Digital Identity environment possible, a charging framework may also include any additional cyber security measures necessary to provide protection, with a particular focus on those required at certified identity providers, for entry into the ecosystem.

It is also common that flexible charging mechanisms be applied, with most recent models related to the number of authentication events, rather than any annual or fixed charge rate mechanism.

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

IBM Security is one of the largest cyber security companies and monitors systems, data and applications across deployed web applications. Cyber-crime can originate from both inside and outside of a corporate information technology environment. In the case of fraud that originates from the public internet, very sophisticated systems (of global scale) are required in order to detect fraudulent attempts to access threats. These systems are in operation today, mostly in banking internet banking environments. IBM would recommend that any party that is participating as an identity provider be required to implement mission critical fraud detection capability. Interconnected systems like these are subject to intrusion attempts by adversaries, who will target and find the weakest link. The damage caused by interconnected and federated systems such as this is disproportionately higher.

Rights and responsibilities need to be clear to all stakeholders. There should be clear accountability and transparency around the roles and responsibilities of identification system providers with a clear third-party Incident Response Planning hierarchy.

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

In cases where it could be proven that their actions resulted in other users being exploited within the system, with that exploitation leading to widespread Digital Identity fraud. For example, if a Relying Party is breached and as a result of that breach, an adversary is able to hijack other user accounts, then the RP should be liable for the consequences.

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?

There are always malicious actors with nefarious aims seeking to access, control and steal large datasets such as this system. IBM would recommend that any detection and response capability across the ecosystem provides the ability for the government to instruct individuals on the nature of any problem, as well as recommendations for remediation. The Australian government has a range of redress and remediation schemes operating and should draw on its own risk profiles, and frameworks to determine remedies and redress based on its experience and categorisation of events. It should also consider directing the provider involved in any breaches to be required to sign up to minimum obligations to assist individuals who are victims of the breach.

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

Proactive notification of fraudulent activity on a user's end point systems should be a feature of the system. The widespread adoption of the Digital Identity system will be enhanced by an overarching and proactive fraud monitoring service. These services act as a proactive alerting mechanism for both the government, in terms of detection of cloned website attacks, and consumers in terms of detection of nefarious content running on endpoint systems. Having a sophisticated fraud capability present across the ecosystem, and specifically on identity providers will drive greater trust and transparency as threats are discovered, mitigated quickly and made transparent to any users.

A world class threat detection and response program that monitors the Digital Identity ecosystem is necessary. Any threats detected across the ecosystem should provide an opportunity to engage the user of such threats. This might include providing the user with remediation options in order to remediate end point systems of adversary content that can lead to identity-oriented loss.

Inclusion and non-discrimination should be observed throughout the system and appropriately be remedied or redressed including those at risk noted in the paper as relying on others to access the system on their behalf. Vulnerable populations are potentially at risk and should be able to access an escalated investigation if they are the victim of fraud, or cyber threats.

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

There is universal recognition of the fundamental importance, and enduring relevance, of the right to privacy and of the need to ensure that it is safeguarded, in law and in practice. It is therefore clear that privacy and consumer protections should include the prohibition of profiling of individuals. IBM believes that the definition of profiling and the purposes of doing this need to be clearer in the legislation.

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

A global context needs to ensure alignment with a risk based approach including use of open source, consensus-driven assurance frameworks and technical standards for digital identification systems. The DTA needs to aim for a high level of assurance and compliance in legislation but also in relevant frameworks such as PSPF/ISM/NIST/ISO etc increasing the level of confidence in the reliability of the digital identity system and its components. As digital identification technologies continue to evolve, leadership, review cycles and governance is critical to ensuring that this system continues to deliver on its potential while protecting human rights and aligning with regulatory and compliance frameworks.

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

Global and interconnected threat and fraud management systems use big data analytics to detect nefarious behaviour on systems and browsers. There is an exclusion listed in this section, which makes it clear that identity fraud systems are exempt. This is important so as to not limit the ability to use effective fraud mitigation techniques used by commercial solutions. In the global fight against internet-based fraud, commercial methods for providing protection may recognise real time, global adversary behaviour through the analysis of endpoint systems connecting to web services.

For further information contact:

- Kaaren Koomen AM, Director of Government & Regulatory Affairs IBM ANZ
- kaaren@au1.ibm.com

- Chris Hockings, IBM Cyber Security CTO.
  hockings@au1.ibm.com

- Kylie Watson, IBM Cyber Security and Cloud Advisory Partner
  kylie.watson@ibm.com

- Nathan Young, IBM Cloud Advisory, Associate Partner.
  nathan.young@ibm.com

28 Sydney Ave,
Forrest, ACT 2603
Australia
www.ibm.com
Ph: 13 24 26.