BixeLab Submission to Senate Standing Committees on Economics

Inquiry into Digital ID Bill 2023 and the Digital ID (Transitional and Consequential Provisions) Bill 202

About us

BixeLab (Biometrics Identity eXperience and Evaluation Laboratory) specialises in testing, compliance, and certification for identity and biometric solutions.

BixeLab is already involved with Australian digital identity testing for a range of organisations. We have an experienced and well qualified team based in Canberra and our testing process meets internationally recognised standards, ensuring that tested biometric systems are put through the most comprehensive and reliable evaluations to identify vulnerabilities and assure performance.

BixeLab (https://BixeLab.com/) is the only ISO certified biometrics testing laboratory in the southern hemisphere and one of only three globally.

Introduction

BixeLab support the objectives of *the Digital ID Bill* and *the Digital ID (Transitional and Consequential Provisions) Bill* in seeking to ensure Australians are in control of their Digital IDs and that their Digital IDs are safeguarded.

Issues

1 Clause 28(2)(d) of the Bill properly identifies the importance of testing to assure that the protection of Digital IDs is effective.

> **28 Accreditation Rules**
> (1) The Accreditation Rules must provide for and in relation to matters concerning the accreditation of entities.
> (2) Without limiting subClause (1), the Accreditation Rules may deal with the following matters:
> …
> (d) without limiting paragraph (c), standards relating to the testing of the information technology systems of entities; …

Under the proposed framework, the requirements for testing will largely be determined by Rules developed by the Regulator, giving flexibility for change in a dynamic environment in response to the adoption of new technologies and the emergence of novel threats. BixeLab agrees that this flexibility is a desirable feature.

2 The current Clause 28(2)(d) (and Clause 81) leaves to the Rules and the discretion of the Regulator (and Systems Administrator) the question of whether and when independent testing might be required. BixeLab believes that it is essential that attribute service providers, identity exchange providers, identity service providers and entities that provide, or propose to provide, services of a kind prescribed by future Accreditation Rules should be subject to independent testing against national and international standards, where they are available and appropriate. The committee may wish to consider an amendment to Clause 28(2)(d) to make explicit that testing of information technology systems may be prescribed to be independent of accredited entities.

3 Testing regimes for evaluating the demographic fairness (sometimes characterised as racial bias) of biometric algorithms have been developed and adopted (e.g. in the United States by the National Institute of Standards and Technology (NIST)). These regimes provide an objective basis for assessing the demographic fairness of algorithms, their training datasets, and their real-world applications. The ban on collection of racial or ethnic attributes contained in Clause 44(1) will prevent testing that might otherwise have been authorised under Clause 49(6). While this no doubt an intended feature of the Bill, it will have the consequence that claims of the demographic fairness or otherwise of the biometric elements of the Digital IDs of Australians will likely be unable to be objectively determined and as a result continue to be the subject of what may be misinformed speculation and commentary.

4 Clause 49(6) authorises retention of biometric data by accredited entities for testing but Clause 51(4) and (5) limit retention to a maximum of 14 days. BixeLab's extensive experience in this field is that 14 days is not a sufficient period to complete testing and associated fraud investigations for more complex and novel threats and attacks. BixeLab suggest the maximum period specified in Clause 51(4) and (5) should be extended to at least 28 days, and preferably to 60 days.

5 Clause 81 provides an authority for the Systems Administrator to approve testing entities, inter alia, for a maximum period of 3 months. BixeLab's extensive experience in cyclic testing relationships suggests that 3 month's is too short a period and that a longer period would be justified for testing entities that can demonstrate accreditation to appropriate international and national standards, as determined by the Systems Administrator.

6 Separately it is not clear how whether testing entities approved under Clause 81 nevertheless remain subject to a separate process of appointment as an accredited entity by the Regulator under point 5 in the table in Clause 59, and therefore subject to the other obligations that follow from this status. The apparent ambiguity is not resolved by the explanatory memorandum.

7 The international standards ISO/IEC 17025 (General Requirements for Competence of Testing and calibration laboratories); ISO/IEC 19795 (biometric performance testing); and ISO/IEC 30107 (Biometric presentation attack detection (PAD) testing), amongst others, are examples of mature standards that express international best practice. Clause 167(2) of the Bill provides a mechanism for incorporating international standards, with or without amendment, into the Rules, including in relation to testing standards. BixeLab agrees that a standards-based approach to testing provides the best possible assurance of protection of Digital IDs and that several existing standards should be adopted.

Conclusion

BixeLab looks forward to continuing its longstanding contribution to improving the Australian digital identity landscape.

Our Canberra-based CEO and founder Dr Ted Dunstone (https://BixeLab.com/ted-dunstone/), a world-renowned biometric, security and AI expert, is available to give evidence to the committee as and if required.