NEC \Orchestrating a brighter world

Trusted Digital Identity Bill, 2021

Exposure Draft Consultation

Digital Transformation Agency

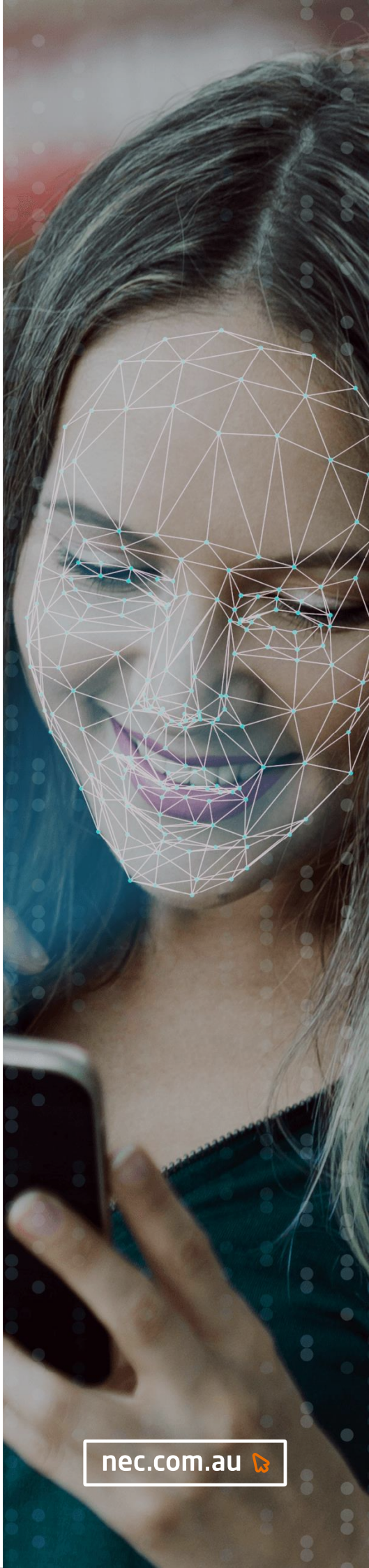
27 October 2021

Version: *3.3*

Date: *27/10/2021*

Author: *Sylvia Jastkowiak, Senior Consultant, Privacy & Security, Business Technology Advisory*

Email: sylvia.jastkowiak@nec.com.au ***Tel:*** +61 450 970 433



NEC would like to thank the Hon. Stuart Robert MP and the Digital Transformation Agency (DTA) for the opportunity to review and comment on the Exposure Draft for the Trusted Digital Identity Bill (2021). We believe continuous industry consultation and dialogue, even once the legislation is passed in Parliament, is important and critical to ensuring public trust moving forward. We recognise that the Digital Identity System will be a dynamic landscape, developing as the system becomes more widespread, as technologies mature and public expectations grow. In order to foster the best development possible for the ever-changing ecosystem, continued dialogue and consultation will be critical in ensuring interoperability between approved entities and cooperation with the Oversight Authority.

We look forward to seeing how the Exposure Draft continues to be developed into robust legislation and would welcome the opportunity to support this submission with further engagement.

Review

The following is a consolidated review of the potential implications and areas of concern for 'accredited entities' (as per the definition on p. 5, Chapter 1, '*Interpretation*' Part 2, Section 9) taking part as participants and identity service providers within the Digital Identity System. NEC has highlighted areas of potential negative/difficult implication and/or sections of the exposure draft that could be further clarified.

Onboarding of Applicants – Onboarding Timeframe

P. 21, Chapter 2, Part 2, Division 2, Section 18, 6c: Successful applicants deemed to be 'accredited entities' receive a notification from the Oversight Authority Body as to the conditions of onboarding onto the system. One such condition is the length of time taken by an entity to onboard. It is stipulated that it only takes an entity to onboard one working day. This condition is again referenced in Section 22, 1c (p. 23). As it will be a condition set out in writing by the Oversight Authority, if the condition is not met (due to technological restraints or other) penalties can be imposed as per p. 22, Section 21, 2. Without understanding all the technical requirements of the System and the inherent implications for accredited entities (this information has not yet been released) it is possible that entities will require more time to onboard, test their functionality and interoperability within the system, before being ready to provide their defined services in an efficient and reliable manner.

P. 21, Chapter 2, Part 2, Division 2, Section 19: Definition of the term '*to be taken*' is requested. Section 19 and its purpose is very unclear without definition (or rewording of this section could also take place).

Notice Before Changes to Conditions on Approval

P. 27-28, Chapter 2, Part 2, Division 2, Section 25, 1-4: Protections to keep the Oversight Authority from changing onboarding conditions for approved entities presents as a concern. A clause requiring the Oversight Authority to provide written notification of entity's approval status and conditions for operation is unfortunately not reassuring protection. Time, economic investment as well as cooperation and goodwill between entities and the Oversight Authority could deteriorate. It would be our recommendation that changes to onboarding criteria after approval status has been given should only occur if the changes are due to serious and urgent risks.

P. 28, Chapter 2, Part 2, Division 2, Section 25, 2b: No timeframe is specified for which the entity can respond to proposed changes specified by the Oversight Authority. A minimum timeframe should be enshrined to allow the entity in question fair recourse.

Additional Privacy Safeguards, Using Biometric Information for Preventing or Detecting Digital Identity Fraud

P. 74-81, Chapter 4, Part 2, Division 2, Section 73 - Section 83.

Due to the way in which the digital identity system will operate, real time fraud detection is extremely unlikely. An individual using the digital identity system may have numerous identities within the broader system: between different accredited identity providers or accredited credential service providers, meaning that various identities for one individual can co-exist comfortably within the ecosystem. If the digital identity system allows for an individual to authenticate their identity (in other words: establish their identity) based on a 'live' photograph being linked to other accredited information sources, synthetic digital identity fraud[1] may be potentially common.

[1] Synthetic identity fraud is when an individual takes authentic forms of identification or information (such as a tax file number, Medicare card and number, passport, date of birth etc.) and couples it together with fake information such as a residential address, email, phone number, name etc. in order to obtain lines of credit, access to bank accounts or other illegal services. It is one of the most difficult forms of fraud to monitor and catch because fraudsters can take years to build identity profiles that are robust and contain genuine forms of identification and information. Synthetic fraud is currently the fastest growing type of identity theft in the United States (as reported by the Federal Reserve).

If identity verification takes place utilising other previously established photographic sources (e.g. passport photographs or drivers licences) as long as that document sources is retrieved digitally and is assumed to be correct (because the photograph and it's source has been tested against others within the same originating system, i.e. NSW RMS database uses 1:n biometric facial verification) identity fraud should be minimised. However, if the document utilised for comparison (verification) is incorrect and fraudulent, identity fraud will be potentially 'enhanced' (new services under the false identity will become available).

The way in which the rules for identity fraud prevention and identification, together with data retention, deletion rules and subsequent related penalties (for contravening the established rules) have been established within the Exposure Draft, we believe disincentivises approved entities within the digital identity system to proactively pursue the exposure of identity theft. Burden of proof and reporting of such activities to the Oversight Authority lie on the entities themselves and penalties for contravening any of the rules are costly and of course, to be avoided (unless an entity seeks to risk their reputation and operating costs in investigating false leads. False leads cannot always be avoided when investigating potential criminal activities and entities will not want to expose themselves to errors).

Entities will provide any information they have in relation to identity fraud matters as requested by law enforcement (a reactive measure on the part of entities) in accordance with the rules stipulated on p. 79 Section 81, i.e. law enforcement suspects that a person has committed an offence or law enforcement has begun proceedings against an individual in contravention to Commonwealth, State or Territory law. However, it can also be assumed that once law enforcement is notified of fraudulent acts, substantial harm may have already been committed against individuals and other entities and/or agencies.

Detailed rules for preventing or detecting digital identity fraud have not yet been made public, however, it is likely that approved service providers within the digital identity platform will perform their identity verification services as requested, to the best of their ability and within the accepted parameters of accuracy. It is unlikely that beyond cyber security measures and established operating procedures, identity fraud will be proactively pursued. The prevention and detection of identity fraud will ultimately fall to the responsibility of the Oversight Authority and Law Enforcement (increasing their workloads).

Ministerial Provisions

P. 21-22 Chapter 2, Part 2, Division 2, Section 20, 1-5.

Ministerial provisions could be further enhanced beyond the measures detailed in the 'Minister's directions regarding onboarding'. For contentious services that spark public debate leading to questions of trust and

legitimacy (particularly in biometric authentication and identity processes, be it 1:1 or 1:n matching in future) the Minister could have the authority to not allow biometric identification services for certain sensitive government processes for as long as deemed necessary. This provision would retain a checks and balances approach that already lends itself to the entity accreditation rules to be established by the Oversight Authority.

Red Teaming Exercise

NEC is supportive of the successful progression and development of the Digital Identity System. NEC would like to propose a red teaming exercise together with the DTA, to work through the framework and rules that will govern fraud prevention and detection activities. We believe we can bring an experienced industry and 'entity' perspective to the table based on our experience in other markets around the world. Our knowledge of biometric Digital Identity technologies and solutions through a privacy and security lens could assist the Government with implementation 'fine tuning' and avoid any unintended consequences of the deployment of the digital identity system for all Australians.

About NEC

NEC has delivered world-class technology solutions and services to customers across the globe, for over 120 years. Serving customers for over 50 years in Australia, NEC has built a sophisticated technology and anything-as-a-service company which brings together the best technology and the best people, driving maximum value for IT and networking investments.

NEC connects Governments, Businesses and people through reliable communication infrastructure while also helping to keep communities safe and secure with smart systems and the world's leading biometrics identification technologies. NEC is a founding ICT Partner of the NSW Government, for the co-creation and development of a world-leading Digital Safer and Smarter City environment. Utilising NEC's world-leading Biometrics, 5G, IoT and AI technologies to support the vision of a sustainable circular economy, we are working on initiatives in five major sectors; Digital Government, Public Safety, Aviation, Healthcare and Smart Transportation.

NEC has a century-long history of innovation. From its cornerstone ideal - ***"Orchestrating a brighter world***" - NEC integrates technologies, expertise and ideas from around the world for the benefit of local

Government and business environments. Our focus remains on value co-creation for customers and partners, maintaining a compatible balance between customer needs and societal expectations.

One area where NEC has led the world for over 50 years is in the area of Biometric Digital Identity technologies and solutions. NEC's fingerprint and facial recognition biometric algorithms have been independently assessed by the US National Institute of Standards and Technology (NIST) as the world's most accurate and fastest biometric matching technologies (a position NEC has comfortably held over the past two decades). NIST have now also carefully assessed the most accurate facial recognition algorithms, to find that they have "undetectable" differences between demographic groups.[2]

NEC's biometrics solutions are deployed in over 57 countries to hundreds of customers, including law enforcement agencies, immigration agencies for border control and digital identity solutions such as drivers licence systems. In the commercial and private sector arena, NEC's facial recognition solutions have been deployed in large public venues, such as airports, entertainment and sporting stadiums, for security purposes, including surveillance and access control.

By working with our customers in numerous countries around the world, NEC is acutely aware of the privacy concerns and varying government regulations around the use of biometrics technologies. As a result, our biometrics solutions are continually evolving to ensure compliance with prevailing government regulations in relation to privacy, such as the European General Data Protect Regulation (GDPR). Furthermore, NEC Australia has paved the way in governance and policy surrounding the design and implementation of its solutions and AI-led technologies (including advanced biometric solutions). In 2020, NEC released our company's policy document based on United Nations Human Rights Law (both the *International Covenant on Civil and Political Rights* as well as the *Convention on the Rights of Persons with disabilities*).

[2] NIST found that the most accurate algorithms (which should be the only algorithms used in government spheres) did not display a significant demographic bias. NIST found that some highly accurate algorithms (including two algorithms submitted by NEC) had false-positive demographic differentials so small as to be "undetectable" for one-to-many searches. In comparison, to the false-negative rates under 1 percent for black females and white males among the highest-performing algorithms, the lowest performing algorithms had false-positive rates for blacks and whites, as high as 99 percent (note: any party can submit an algorithm for testing, hence the great disparity and difference between algorithm performance).
Patrick Grother, Mei Ngan, and Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 2: Identification (Washington, DC: National Institute of Standards and Technology, September 2019), 47, https://www.nist.gov/system/files/documents/2019/09/11/nistir_8271_20190911.pdf#page=49.

NEC's Principles (as pictured above) work in harmony together and take into consideration both technical and non-technical attributes of technology and solution design & implementation.

NEC's priorities showcase deep values linked to democracy (participation in civil life), protection and digital inclusion of vulnerable persons and communities, gender equality, access to opportunities (self-actualisation), sanctity of government rule of law as well as legitimacy based on public acceptance. All these values should be present and protected in the Digital Identity System design and Legislation, whilst making the most out of the opportunities that technology presents for a connected and secure digital economy.

NEC \Orchestrating a brighter world

Contact us at:

nec.com.au

or call us on 131 632

Australia	Corporate H.Q. (Japan)	North America (USA)	Asia Pacific (AP)	Europe (EMEA)
NEC Australia Pty. Ltd.	NEC Corporation	NEC Corporation of America	NEC Asia Pacific	NEC Enterprise Solutions
nec.com.au	nec.com	necam.com	sg.nec.com	nec-enterprise.com