NEC \Orchestrating a brighter world

Digital Identity Legislation Response

Consultation Round 2

Digital Transformation Agency

14 July 2021

Version: *Final*

Date: *14/07/2021*

Author: *Sylvia Jastkowiak*

Executive Summary

NEC Australia is supportive of the development to create a Digital Identity System, providing citizens and businesses a means to connect with government services and the digital economy in a streamlined, accessible and convenient manner. NEC advocates for greater emphasis to be placed on the proposed Privacy Impact Assessments to be completed by Trusted Digital Identity Framework (TDIF) Providers. Providers within the Digital Identity ecosystem must have a greater understanding of their privacy, security and ethical obligations in relation to the services they provide for the benefit of citizens.

This submission explains NEC's Human Rights approach to technology design and implementation. This approach would foster tangible effects on the behaviours of providers and participants within the system, creating *trust* whilst inherently addressing and adhering to the Privacy Act (1988), as well as any added security/privacy measures established by the Digital Transformation Agency (but without the need to create overly-complex legislation which can be difficult and costly to enforce).

The second half of our submission encourages the Digital Transformation Agency (DTA) to consider how best to enable one to many facial recognition searches to be conducted on the basis of identity fraud investigations. Securing the digital identities of users and acting on incidences of suspected fraud (relating to the use of facial images) in an accurate and timely manner (before other serious crimes are committed) should be paramount in the obligations and responsibilities of the Oversight Authority body. This stance does not change the one to one facial recognition matching completed for identity verification methods used within the system on a regular basis. Importantly, neither does it change or erode the autonomy and decisions a citizen has when deciding to create or delete digital identities and using available methods of authentication.

General Support

NEC would like to thank the Digital Transformation Agency for the opportunity to contribute a response regarding the Digital Identity System. NEC as a world leading biometric and ICT provider, agrees with many of the proposed legislative and governance framework directives of the Digital Identity System. Namely, that creating and using a Digital Identity is voluntary, multiple digital identity verification pathways can be created for the purpose of accessing different services and the ability to delete a digital identity resting with the user and owner of a digital identity (ensuring their human autonomy over the system and identities created). We also support that in some circumstances, where a government service requires a higher level of security, sensitivity and is an essential service (for example, requiring biometric verification in combination with other personal documentation) an exemption can be applied for in regards to the requirement of providing an alternative channel to Digital Identity to access their service.

Developing and Ensuring Trust & Legitimacy

The requirement to conduct a 'Privacy Impact Assessment' as part of the TDIF accreditation process is also strongly supported by NEC. We consider that this requirement should not simply be part of the accreditation process, but rather, is seen as an opportunity to change cultural awareness in the identity management and technology industry, to safeguard users integrity and freedoms of choice, in an ethical manner. The DTA states in its Consultation Paper that privacy and consumer protections specific to the Digital Identity System are "*to support and encourage trust*" (see section 3.1 Purpose of the Legislation in 'Overview of the Legislation'). Trust in the systems governance and the participation of both government and industry providers cannot rely on legislative controls and protections alone. NEC is in agreement that privacy and security protections should not duplicate the safeguards built into the Privacy Act (1988) in classification of data and it's detailed fundamentals of limitation in collection, usage, storage and deletion[1], however, what the Privacy Act often fails to address is intent and maturity in understanding the implications and impacts of technology design and automated decision making processes (in this case, by identity verification providers and government services). Applying a human rights approach to the oversight and accountability measures surrounding the Digital Identity as a whole (including the Privacy Impact Assessment), and in particular for TDIF providers and Accredited Participants, would increase the publics support of the system[2] and therefore, require less creation of costly and rigid legislation allowing for a more successful implementation (in

[1] As the High Court of England and Wales observed in the first legal challenge to the use of facial recognition technology in 2019: "The fact that a technology is new does not mean that it is outside the scope of existing regulation, or that it is always necessary to create a bespoke legal framework for it." This comment was made in the first major court decision on the use of automated facial recognition technology: Bridges, R v The Chief Constable of South Wales Police, EWHC 2341 (Admin), [84] (Haddon-Cave J, Swift J), 2019

2 In 2020, the Human Rights Commission of Australia engaged Essential Media to undertake polling on trust in the use of AI to make decisions. Over three quarters of respondents said they would have more trust in a system that created automated government decisions, if there were stronger oversight measures that included an understandings and implementation of human rights. Australian Human Rights Commission, 'Human Rights and Technology', Final Report, 2021

acceptance and legitimacy) as well as providing opportunity for additional updates to the system in the future.

NEC Australia has paved the way in governance and policy surrounding the design and implementation of its solutions and AI-led technologies (i.e. biometrics). 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*). Our policy framework takes 10 NEC principles and directly links them to the UN Accords, with tangible directives on the design and implementation of technology. Centred on both specific Articles within the Human Rights Accords, as well as the general understanding and intent of the Human Rights Accords, provides a definition and contextual understanding of said values as well as a risk framework. NEC's global mission is to create and support technology that not only minimises harms and risks to communities and vulnerable groups and/or individuals, but rather goes further by striving to create equality, opportunity and work toward a common good (social value creation).

NEC's priorities showcase deep values linked to democracy (participation in civil life), protection and digital inclusion of vulnerable persons, gender equality, access to opportunities (self-actualisation), sanctity of government rule of law as well as legitimacy based on public acceptance. All of 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'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.

Where conceptual and ideological gaps present themselves between the U.N. Human Rights Accords, and NEC Value and specific technological implications, other globally recognised standards have been consulted (e.g. *E.U. Commission Guidelines on the Ethics in Artificial Intelligence* and the *GDPR*).

NEC's strategy in furthering our privacy and ethical stance on the design and implementation of advanced technologies and solutions in the Australian context has included the release of a Privacy and Ethics Impact

Assessment (PEIA) in 2021 (based on the Human Rights Governance Framework established in the internal policy document and the *Privacy Act*, *1988*) and is available to both Customers as a service, as well as for internal practise. The innovative assessment has tangible impacts on not only the design of the solution, but also our users of the technology. The PEIA is revisited at different intervals in time, so it is regularly updated as solutions and our customers' operating environments undergo change or modifications. For this reason, NEC supports and recommends that TDIF and Accredited Participants are able to complete their own Privacy Impact Assessments, as long as the individual carrying out the assessment for an agency/actor has individual capability, independence and oversight of both the technical and non-technical attributes of a solution.

The Role of Biometrics and Facial Recognition in Digital Identity Legislation

NEC Australia advocates for the use of biometrics to find fraudulent identities within the Digital Identity landscape (whether this occurs at its inception or in further development phases of the Digital Identity System or in its inception). We consider that by giving the users a choice in whether their Digital Identities can be used for fraud investigations, will eliminate the ability of government services (or law enforcement) to catch acts of fraud in a more timely and successful manner. It can be assumed that individuals using the system with ulterior (and criminal) intentions will not allow for their created digital identities to be accessible for criminal investigations. All other user discretion, protections and autonomy for the user would remain (e.g. the user's choice to utilise biometric identification for different services and the choice to delete their digital identity).

In 2018, NEC Australia rolled out one of its facial recognition solutions (NeoFace® Reveal) across NSW's Transport Road and Maritime Services (RMS, later to be rebranded and streamlined into 'Services NSW'). New facial photographs for licences are checked against the broader facial database to make sure duplications are removed and to identify potential fraud. When a duplication exists against another individual's account, the instance is flagged by the system (licence services are thus put on hold). Trained staff review the individuals claim and identity. Services NSW staff utilise the similarity score provided by the NeoFace algorithm as *intelligence* to make an informed decision about the identity of the individual presenting themselves to Services NSW. The solution itself does not make arbitrary decisions (without human oversight). It is also important to note that different levels of readdress exist. Within a short period of RMS utilising the NEC solution and facial recognition algorithm, fraudulent identities were uncovered and confirmed by other government agencies.

A NSW Parliamentary consultative process and inquiry occurred before a Bill to allow facial recognition comparison to be used in transportation and identification services (by RMS/Services NSW) was drafted.[3] It established that identity crime causes substantial harm to the economy and individuals. Identity crime impacts one in four Australians throughout their lifetime, with an annual cost of at least $2 billion.[4] Identity crime enables other serious crimes to be committed, such as offenders using fake identities to purchase

[3] **New South Wales. Parliament**. **Legislative Council. Standing Committee on Law and Justice.** Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018 / Legislative Council, Standing Committee on Law and Justice. [Sydney, N.S.W.] : The Committee, 2018. – [30] pages ; 30 cm. (Report ; no. 65), Chair: The Hon Natalie Ward MLC., Published November 2018.
4 Ibid.

ammunition (e.g. for terrorism related purposes).[5] While Agencies can already verify information on identity documents by using 'the Document Verification Service' (a name-based checking tool) it cannot detect when a fraudulent photo is used with otherwise legitimate documents, or assist in identifying an unknown person from a facial image. The Department of Home Affairs argued that current image-based methods of identifying an unknown person can be slow, difficult to audit and often involve manual tasking between agencies, which can be a lengthy process. For this reason, Home Affairs supported the use of identity-matching services which will streamline these processes by providing authorised agencies with the means to rapidly share and match facial images.[6] The Information and Privacy Commission supported the Government's views that the capability (for Drivers Licence Facial Recognition including one to one matching as well as one to many) was designed to include robust privacy safeguards that measured up to concerns relating to privacy, security and ethics.[7]

One to one facial recognition matching can certainly remain as the core authentication method used when citizens need to prove their identity to access services. However, to catch fraud in real time (or in a timelier manner) and before other damages and crimes are committed, one to many biometric matching should be considered to take advantage of secure and more accurate technology. This matching and searching could can led by law enforcement groups, the Digital Identity Oversight Authority and in conjunction with technology experts (providing there are exclusions in the legislation and the like). Robust governance frameworks and workflows can be developed, in accordance with Privacy Legislation and Human Rights-led ethical standards.

Selected algorithms to perform one to many matching should undergo a vetting process to ensure higher accuracy levels can be achieved and vendors should hold experience in such undertakings (identity authentication services and one to many facial recognition matching). NEC's Neoface® algorithms are routinely independently tested by the National Institute of Standards and Technology (U.S. Department of Commerce: considered to be the global standard for complex and robust algorithm testing worldwide). In 2019, NEC ranked first in the Face Recognition Vendor Test (FRVT) identification (one to many matching), leading the way with an error rate of 0.5% when matching against a database of 12 million people.[8] It should be noted that facial recognition algorithm testing by NIST is conducted every 2-4 years.

---

[5] "The Commonwealth Department of Home Affairs noted the following benefits of the identity-matching services; preventing identity crimes, general law enforcement, national security, protective security, community safety, road safety and identity verification." Submission 1, Department of Home Affairs, p. 3-5. **New South Wales. Parliament. Legislative Council. Standing Committee on Law and Justice.** Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018 / Legislative Council, Standing Committee on Law and Justice. [Sydney, N.S.W.] : The Committee, 2018. – [30] pages ; 30 cm. (Report ; no. 65), Chair: The Hon Natalie Ward MLC., Published November 2018.

[6] **New South Wales. Parliament. Legislative Council. Standing Committee on Law and Justice.** Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018 / Legislative Council, Standing Committee on Law and Justice. [Sydney, N.S.W.] : The Committee, 2018. – [30] pages ; 30 cm. (Report ; no. 65), Chair: The Hon Natalie Ward MLC., Published November 2018.

[7] Submission 2, Information and Privacy Commission, p.2. Ibid.

[8] "49 organizations, including companies from the United States, China, Russia, Europe, and Japan, participated in the NIST's FRVT 2018 (published and announced 2019) where the evaluation of face recognition accuracy was performed. These tests are the most rigorous and fair benchmarks implemented by the NIST…By performing multi-stage matching, an impressive search speed of 230 million matchings per second was achieved. Furthermore, leveraging NEC's deep learning methods to significantly reduce the identification error rate, NEC accurately matched images of a subject taken over a 10-year interval with an error rate that was 4 times lower than the runner-up.", 'NEC Software Solutions UK, Insights: NEC tech ranked No. 1 in NIST tests', https://www.necsws.com/news/nec-facial-recognition-ranked-top-in-nist-tests/ 30th October 2019

NEC Australia recommends that the Digital Identity System being developed by the Australian Government takes advantage of accurate, fast and secure biometric technology, which will only enhance the security landscape of digital identities (fundamentally protecting the digital identities of citizens). Created with an excellent understanding of solution processes and AI, alongside human rights led privacy and governance frameworks, we can only further the goals and aims of this future-thinking project, to serve citizens legitimately and positively, whilst creating trust and legitimacy between government, providers and the general public.

NEC welcomes the opportunity to discuss this submission in person. Thank you for the opportunity to contribute to this important policy development.

About NEC

NEC's mission: Orchestrating a brighter world, solving tomorrow's technology challenges today. NEC is committed to creating value for all members of society, believing that with technology and co-creation, digital solutions can address society's needs.

Established in 1899 (120 years ago) NEC is one of the world's leading technology companies. During its long history, NEC has consistently been ranked among the world's most innovative companies and is the company widely regarded as leading the world in the integration of computers and communications, coining the logo C & C.

NEC Australia was established in 1969. During this period NEC has been a major contributor to the country's telecommunications and business communications. In 1996, NEC introduced the *world's first* digital mobile phone and in 2008, NEC Australia revolutionised the classroom with the introduction of interactive whiteboards across the education sector. Over the past two decades the company has evolved into a dynamic ICT and IT services company.

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. 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 entertainment and sporting stadiums, for security purposes, including surveillance and access control.

In more recent history NEC has developed solutions using its facial recognition technology to provide solutions to enhance the customer experience and address the societal issues associated with an ever growing population, such as frictionless fast passenger processing systems in airports that allow a passenger to move from "curb to gate" using their face as their "ticket", providing a contactless experience. In this way

we will continue to be bold, ambitious, driven, and the leading provider of intelligent solutions in biometrics, facial recognition, cyber and surveillance security.

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 Japan has established a Digital Trust Division within the company, to regulate and control the deployment and use cases of its biometrics and digital identity technologies and solutions to ensure that they meet prevailing legal regulations in each country, as well as ensuring the appropriate use of these technologies are in line with NEC's human rights principle and values towards providing solutions for society that enhance safety, security, efficiency and equality.