APPI
Australian Public Policy Institute

Policy Insights Paper

Improving governance and training for the use of facial verification technology in NSW Digital ID

Professor Edward Santow, Sophie Farthing
and Lauren Perry

November 2023

Contents

Acknowledgement of Country

The James Martin Institute for Public Policy acknowledges the Gadigal people of the Eora Nation upon whose ancestral lands our Institute stands.
We pay respect to Elders both past and present, acknowledging them as the traditional custodians of knowledge for these lands.
We celebrate the diversity of Aboriginal peoples and their ongoing cultures and connections to the lands and waters of NSW.

About the JMI Policy Challenge Grant

The James Martin Institute for Public Policy (JMI) is a unique joint venture between government and leading Australian universities. Launched in 2021 as a formal partner of the NSW Government, we work closely with government ministers, departments, and other decision-makers to help address their most pressing policy priorities, enabling them to harness a wide range of expert advice. JMI is an independent, non-partisan policy institute with charitable status.

This paper was made possible through a JMI Policy Challenge Grant. This annual grant program supports academics who seek to tackle the greatest public policy challenges facing Australia.

About the authors

Professor Edward Santow is the Director - Policy & Governance at the Human Technology Institute (HTI), and Industry Professor - Responsible Technology at the University of Technology Sydney (UTS).

Sophie Farthing is a human rights lawyer and public policy expert with extensive experience across Australia and the UK. She is Head of the Policy Lab at HTI.

Lauren Perry is the Responsible Technology Policy Specialist at HTI, with a background in public policy and social and political sciences.

About the Human Technology Institute

The Human Technology Institute (HTI) is building a future that applies human values to new technology. HTI embodies the strategic vision of UTS to be a leading public university of technology, recognised for its global impact specifically in the responsible development, use and regulation of technology.

HTI is an authoritative voice in Australia and internationally on human-centred technology.
HTI works with communities and organisations to develop skills, tools and policy that ensure new and emerging technologies are safe, fair and inclusive and do not replicate and entrench existing inequalities.

The work of HTI is informed by a multi-disciplinary approach with expertise in data science, law and governance, policy and human rights. To support its engagement with Service NSW in this project, HTI drew on several of its major projects, including in relation to facial recognition technology; independent expert advice provided to Services Australia in relation to the recommendation in the MyGov Independent User Audit to establish myGov in framework legislation; and independent expert advice provided to the NSW Government regarding the NSW AI Assurance Framework.

Acknowledgements

HTI would like to thank the Service NSW Digital Identity and Inclusive Journeys teams for their collaboration throughout the project.

Authorship

The findings and recommendations of any JMI publication are solely those of its authors, and do not necessarily reflect the views of JMI, its Board, funders, advisers, or other partners.

Disclaimer

Professor Santow is a member of the NSW Government AI Review Committee. All advice provided to Service NSW in the context of this JMI project is independent of any interactions between the agency and the NSW AI Review Committee.

Executive summary

Modern life is almost impossible if you cannot prove who you are. Verifying one's identity is essential for employment, to access government services and to engage with a range of companies. This is unlikely to change.

In the analogue world, we assert our identity with paper documents using a passport, driver's licence, or birth certificate. The public and private sector organisations that we interact with keep records of these documents, and adopt error-prone, privacy-intrusive and expensive processes in the identity verification process.

The rise of digital identity is transforming these analogue processes. **Digital identity initiatives involve the use of new technology to verify individuals' identity.** Done well, this can increase convenience for citizens, reduce privacy and other risks, and save money for government and the private sector. However, **digital identity brings its own risks that must be understood and addressed** in order to realise the promise of a more secure and effective way of verifying people's identity.

New South Wales has been leading the way – compared with other Australian jurisdictions, and also many other nations – in the digital transformation of government services. **In April 2022, the NSW Government committed to establishing a Digital ID for the people of NSW.** This program aims to make it safer and more convenient for people to complete identity-based administrative tasks while handing back greater control to individuals of their digital identity and credentials.

> ***With the world moving towards a digital future, it's more important than ever for people to feel safe when providing personal information online and the Digital ID will help do just that.***
>
> *The Hon. Jihad Dib MP, NSW Minister for Customer Service and Digital Government*[1]

The NSW Digital ID system includes the use of facial verification technology (FVT) and liveness detection, a type of facial analysis technology. These are powerful technologies that can be deployed to create a convenient and secure system of identity verification. However, as examples of a broader class of facial recognition technology (FRT), they also pose risks for human rights such as privacy, non-discrimination and access to social security.

Without effective protections, individuals are at risk of harm, and community trust in government can be undermined. As Service NSW develops authentication and verification processes for Digital ID, there is **a need to ensure that appropriate regulatory and governance systems protect NSW citizens** and build a firm foundation of trust and public benefit.

With the backing of a JMI Policy Challenge Grant, the Human Technology Institute (HTI) collaborated with Service NSW to develop independent expert advice that **proposes a governance framework and training strategy to support Service NSW and the Department of Customer Service in its development and rollout of a safe, reliable and responsible digital identity and verifiable credentials (DIVC) system.**

HTI's proposed governance framework contains ten principles to inform supporting legislation and policy for NSW Digital ID:

Box 1

Ten principles to inform supporting legislation and policy for NSW Digital ID:

1. NSW Digital ID should be established in law.
2. NSW Digital ID should protect and promote the privacy and data security of all users.
3. There should be independent monitoring and oversight of NSW Digital ID.
4. Legislation and policy for NSW Digital ID should ensure citizen autonomy through effective mechanisms for choice and consent.
5. NSW Digital ID should perform to a high standard of accuracy and be fit for purpose. Service NSW, as the responsible agency, should report publicly and periodically on relevant independent benchmarking and technical standards compliance.
6. NSW Digital ID should be useable for all, with the benefits enjoyed by everyone equally.
7. Service NSW, as the responsible agency for NSW Digital ID, should put in place robust internal monitoring and oversight mechanisms.
8. NSW Digital ID users should be able to access timely correction and redress.
9. There should be clear communication to the public about NSW Digital ID prior to its rollout.
10. NSW Digital ID should be developed with a view to integrating with federal and other Australian digital identity systems.

HTI's proposed training strategy aims to **support all relevant staff to understand the risks, responsibilities and appropriate responses** to issues likely to arise in respect of the NSW Digital ID system. It proposes a three-tiered approach applying to senior executives, operational staff and decision makers, through to customer-facing representatives.

This Policy Insights Paper also **reflects on this process of collaborative policymaking** and presents **key recommendations for best practice governance and training** in relation to the development and rollout of government digital identity initiatives. We observe the challenges in developing data and artificial intelligence (AI)-enabled tools for government service delivery, with the aim of solving complex privacy and security problems while improving the lives of citizens.

HTI's process involved drawing on expert knowledge and community consultation. Through Service NSW's openness to engaging independent experts like HTI, the agency is working to ensure its DIVC systems are not just user-friendly but also rooted in **a strong legislative framework and training strategy.** Through this approach, the NSW Government is on its way to adopting a world-leading, trustworthy and high-quality digital identity system.

Introduction

In April 2022, the NSW Government announced it would establish a digital identity system for NSW customers.[2] The digital identity initiative — NSW Digital ID — implemented by Service NSW, aims to make it safer and more convenient for people to complete identity-based administrative tasks, while giving greater control to individuals of their digital identity and credentials.[3]

While digital identity technology promises great benefits in terms of user convenience and enhanced security for personal information, it also carries significant risk if personal information is compromised. The risk of harm is even more significant when digital identity relies on biometric information — as is the case with NSW Digital ID — to verify an individual is who they say they are.

Supported by a JMI Policy Challenge Grant,[4] HTI has worked collaboratively with Service NSW to provide independent expert advice regarding two elements of the safe and accountable rollout of digital identity in NSW. HTI has:

1. Developed a governance framework, setting out ten principles to underpin regulation for digital identity products and services in NSW.
2. Produced a training strategy, adopting a three-tiered approach to educate and upskill Service NSW employees, from the senior executive leadership through to frontline service delivery staff.

HTI set out its detailed independent expert advice for Service NSW in October 2023.

In this Policy Insights Paper, HTI distils some key insights from the collaborative process it undertook with Service NSW to develop the governance framework and training strategy, and summarises the independent expert advice provided to Service NSW.

Project outline

HTI and Service NSW shared the goal of ensuring that facial verification technology is safely developed and deployed in NSW. Prior to receiving the JMI Policy Challenge Grant, HTI provided some informal advice to Service NSW on this initiative.

The JMI grant, awarded in late 2022, helped to formalise HTI's work with Service NSW. In a series of meetings between December 2022 and July 2023, HTI and Service NSW discussed:

- the proposed design and rollout of NSW Digital ID, including technology design and pilot testing;
- the development of the governance framework, including the policy underpinnings for proposed legislation; and
- training requirements for Service NSW staff, as well as the role of community education.

The primary project output was written independent expert advice from HTI, outlining the governance framework and training strategy, which was provided to Service NSW in October 2023.

Digital identity in Australia

What is digital identity?

Digital identity refers to digital technology that can verify a person's identity and their key credentials in order to enable the individual to engage in transactions for goods and services without the need for face-to-face interactions, physically-sighted documents, or the proliferation of digital copies of sensitive information.

Globally, there is a shift towards using digital identity systems to underpin how citizens interact with governments. Such systems can improve how individuals engage with government and corporations. With strong technological, legal and service delivery foundations, the move towards digital identity can deliver increased convenience, improve privacy protections and the security of personal information, and make government and business more efficient.

However, digital identity also carries significant risk (see Box 2 below). Technology that enables digital identity initiatives – especially facial recognition technologies (FRT) such as facial verification, facial identification, or facial analysis – unavoidably restricts the right to privacy. Recent major data breaches, involving millions of Australians, remind us of the consequences of poor data practices.

Therefore, there is a strong public expectation that government must do better to protect the privacy and security of personal information. Comparable jurisdictions, such as the United Kingdom, have recognised these risks and are moving to legislate for digital identity. The UK's Data Protection and Digital Information (No. 2) Bill (before the House of Commons, at the time of writing) underpins the governance structure and privacy, security and accessibility standards for the UK digital identity and attributes trust framework.[5]

In Australia, NSW was the first Australian jurisdiction to develop a digital identity solution for residents. Since the NSW Government's announcement that it would develop NSW Digital ID, there have been several key policy developments, including a national commitment to developing digital identity across every Australian jurisdiction. For example:

- In June 2023, the Australian Government published a National Strategy for Identity Resilience, articulating a national commitment to build a resilient digital identity system "that enables smarter, safer and more effective service delivery".[6]
- In September 2023, the Identity Verification Services Bill and the Identity Verification Services (Consequential Amendments) Bill were introduced to the Australian Parliament, proposing legislative underpinning for many of the pre-existing identity verification services which are increasingly relied on in digital identity verification processes.[7]
- In late November 2023, the Digital ID Bill 2023, and the Digital ID (Transitional and Consequential Provisions) Bill 2023 were introduced to the Australian Parliament to support the Australian Government Digital ID system to become a nationally regulated, whole-of-economy system.[8]

The NSW Government has an opportunity to lead by example through best practice technology design, policy development and supporting legislation for digital identity. The project undertaken by HTI, culminating in the independent expert advice provided by HTI to Service NSW, aims to support this ambition.

Box 2

Risk of harms posed by the use of Facial Verification Technology and liveness detection in digital identity

Facial recognition is a relatively new technology, with ongoing work by governments and technical experts to assess the performance of various FRT applications in identifying individuals. Given the imperfect nature of these technologies, and the ways they interact with a person's sensitive personal information and legal identity, there are a range of risks for users. This is especially true when such technology is used to make decisions that affect people's legal and similarly significant rights. Such risks include:

- algorithmic bias and errors, including demographic variations in error rates, which can lead to discrimination, misidentification or failure to identify an individual;
- denial of access to basic services and entitlements;
- data aggregation of sensitive personal information;
- risk of identity fraud or hacking of personal information;
- lack of transparency or accountability for administrative decision-making; and
- loss of trust in government.

HTI's 2022 report Facial Recognition Technology: Towards a model law provides a detailed analysis of the risks of FRT and proposes a model law be developed to ensure the use of FRT upholds human rights.[9]

NSW Digital Identity

The NSW Government has committed to providing all Service NSW customers with a digital identity. The NSW Government's Digital Identity Strategy, implemented by Service NSW, aims to improve customer service and personal data security while increasing access to government services for citizens.

A key initiative of this strategy is **NSW Digital ID, an online and app-based service that aims to simplify the process of proving identity in a range of contexts,** such as renewing a Working with Children Check or buying alcohol online. While NSW Digital ID offers a new, simpler way to verify identity or access government services in NSW, it will not replace existing alternatives.

NSW Digital ID will be enabled through the following key authentication and verification processes:

1. Authentication of a user by unlocking their smart device with their face using a self-provided image. This face-capture process is not checked against an external source database. (Note that users also have the option of authenticating themselves via other means such as a PIN code).
2. 'Liveness detection', which uses biometric analysis including three-dimensionality checking to ensure that the person being verified is a genuine individual requesting the service in real time.[10] Liveness detection aims to address some types of fraud, such as the use of hyper-realistic masks based on another individual's face.
3. One-to-one matching of a face against an externally-held reference image of that same face, also referred to as facial verification technology (FVT).

This process is presented in further detail in Figure 1.

Verification of digital identity using facial verification technology

Traditionally, verification tools have included username and password combinations or multi-factor authentication applications. However, increasingly, FVT and other biometric technologies are being used as quick and convenient methods to verify an individual's identity using the unique 'credential' of their face. The use of facial verification for digital identity authentication is often claimed to be more secure, less susceptible to identity fraud, and more convenient for customers.[11] Service NSW refers to digital identity enabled by FVT as:

> *a way to prove your identity in a safe and secure way when accessing services or completing transactions online or in-person. A digital identity removes the need to prove your identity through face-to-face interactions and by using physical identity documents.*[12]

Facial verification is sometimes referred to as 'one-to-one' matching, as it involves matching the data from a face image to a pre-existing, validated record of that same face. This technology is most commonly used when unlocking personal smart devices and in immigration processing at airport 'eGates'.

Security measures such as liveness detection

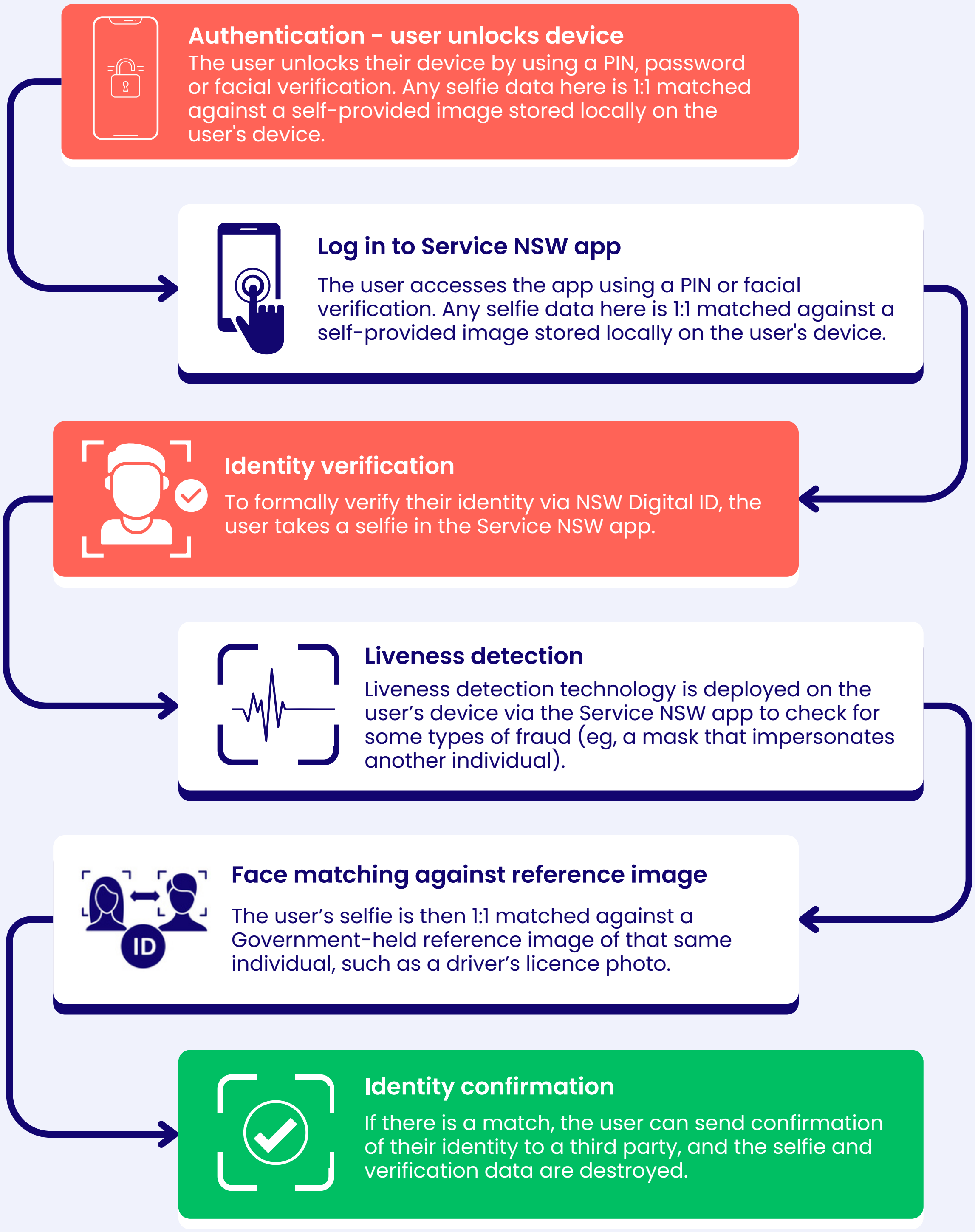
For any digital identity systems that use facial verification technology, other security measures can, and should, be included to enhance the security of the system. This could include additional authentication using PIN codes or passwords.

The NSW Digital ID relies especially on facial analysis for liveness detection. Many forms of facial analysis carry high risks and can have low rates of accuracy.[13] The consensual use of this technology in a controlled environment purely to assist in the prevention of identity fraud and promotion of security of personal information is justifiable, provided effective safeguards are in place.

While the precise performance (or accuracy) ratings of the NSW liveness detection solution are not publicly available, the effectiveness of such measures is crucial to the safety and successful operation of the system. There is an ongoing need to monitor the effectiveness of such security measures over time, given that this is a dynamic area of fraudulent activity, and criminals have an interest in finding new ways to unlawfully access digital identity systems.

Figure 1

The user authentication and identity verification process – NSW Digital ID



Authentication - user unlocks device
The user unlocks their device by using a PIN, password or facial verification. Any selfie data here is 1:1 matched against a self-provided image stored locally on the user's device.

Log in to Service NSW app
The user accesses the app using a PIN or facial verification. Any selfie data here is 1:1 matched against a self-provided image stored locally on the user's device.

Identity verification
To formally verify their identity via NSW Digital ID, the user takes a selfie in the Service NSW app.

Liveness detection
Liveness detection technology is deployed on the user's device via the Service NSW app to check for some types of fraud (eg, a mask that impersonates another individual).

Face matching against reference image
The user's selfie is then 1:1 matched against a Government-held reference image of that same individual, such as a driver's licence photo.

Identity confirmation
If there is a match, the user can send confirmation of their identity to a third party, and the selfie and verification data are destroyed.

Summary of HTI's independent expert advice to Service NSW

A governance framework for NSW Digital ID

A strong governance framework is crucial in supporting the safe and responsible rollout of NSW Digital ID. By 'governance', we mean legislation to uphold customer rights and protections, robust policy on how digital identification is used and deployed, and departmental guidance on best practice approaches for working with staff and customers.

HTI's proposed governance framework is centred on ten principles that aim to build trustworthiness in NSW Digital ID by:

- supporting inclusive and accessible digital identity;
- upholding relevant human rights, including strong protections for the right to privacy; and
- promoting resilient and robust digital identities.

Principles to inform the governance framework for NSW Digital ID

1. **Legislation for digital identity:** NSW Digital ID should be established in law.

2. **Privacy and data security:** NSW Digital ID should protect and promote the privacy and data security of all users.

3. **External regulatory oversight:** There should be independent monitoring and oversight of NSW Digital ID.

4. **Consent and autonomy:** Legislation and policy for NSW Digital ID should ensure citizen autonomy through effective mechanisms for choice and consent.

5. **Performance standards and reporting:** NSW Digital ID should perform to a high standard of accuracy and be fit for purpose. Service NSW, as the responsible agency, should report publicly and periodically on relevant independent benchmarking and technical standards compliance.

6. **Accessibility, inclusion and user-centricity:** NSW Digital ID should be useable for all, with the benefits enjoyed by everyone equally.

7. **Internal monitoring and oversight:** Service NSW, as the responsible agency for NSW Digital ID, should put in place robust internal monitoring and oversight mechanisms.

8. **Correction and redress:** NSW Digital ID users should be able to access timely redress mechanisms.

9. **Public education about NSW Digital ID:** There should be clear communication to the public about NSW Digital ID prior to its rollout.

10. **Interoperability:** NSW Digital ID should be developed with a view to integrating with federal and other digital identity systems.

A training strategy for Service NSW

Alongside a robust governance framework, HTI has proposed a NSW Digital Training Strategy which would ensure all staff involved in DIVC — from senior executives, through to customer-facing representatives — understand the risks, responsibilities and appropriate responses to issues likely to arise in respect of the NSW Digital ID system. It should improve the knowledge and skills of employees in different roles across the agency through targeted training around the safe development, deployment and governance of NSW Digital ID products and services.

As highlighted by several recommendations from the Royal Commission into the Robodebt Scheme, training in relation to a particular government service should not be restricted to just those who are responsible for face-to-face delivery; role-specific training should be provided to all employees connected to the service. This includes senior executive leaders as well as managers overseeing project teams.

This training strategy should be fit for the current stage of NSW Digital ID products being rolled out, as well as adaptable to change and improvement as the DIVC portfolio continues to expand and new products and services are offered to the community.

Recommended training program for Service NSW staff

HTI proposes that digital identification training be tailored to three broad cohorts within Service NSW:

Level A – DIVC strategic leadership workshop

Participants and format	Content
A one-off, 1-2 hour workshop. Leadership workshops are best delivered in-person for 8-16 executive staff across Service NSW and the Department of Customer Service with high-level responsibilities for DIVC strategy, including digital service delivery, governance and legal oversight.	Core topics for Level A training could include: • Understanding digital identity, FVT and liveness detection. • Mitigating risks of the DIVC program from strategic, governance and regulatory perspectives. • Ensuring workforce preparedness for DIVC rollout. • Towards a successful future for DIVC – integrating risk and compliance frameworks.

Level B – Responsible DIVC development and oversight masterclass

Participants and format	Content
A one-off, 3 hour masterclass. The masterclass can be delivered either in-person or remotely for around 12-24 professional staff with management and operational responsibilities.	Core topics for Level B training could include: • Deepening understanding of DIVC risks and opportunities for Service NSW and its customers, and how to address them. • Maintaining compliance with changing legal, policy and ethical standards (with particular attention to the NSW context). • Responsible design and procurement principles. • Responding to privacy and cybersecurity threats. • Embedding accessibility and inclusive design processes into DIVC products. • Identifying when things are going wrong with the products, including system-wide anomalies, and escalating concerns. • Ensuring proactive oversight and governance of DIVC systems. • Supporting frontline customer service staff.

Level C – DIVC fundamentals for frontline staff	
Participants and format	**Content**
A one-off, 1 or 2 hour, in-person training course. This could be delivered for a relatively large cohort of frontline workers in a designated training room environment.	Core topics for Level C training could include: • Introduction to NSW Digital ID policy, products and services. • Explaining the nature, risks and benefits of DIVC products (including FVT and liveness detection) to Service NSW customers. • Providing accessibility support for customers with disability or other access requirements. • Identifying when things are going wrong with the products (including one-off, customer-based experiences, as well as broader system-wide anomalies), and escalating concerns. • Guiding customers through complaint escalation and possible redress mechanisms.

Policy insights

Applying a socio-technical approach to new technologies

HTI adopts a socio-technical approach to the use of new and emerging technologies. That is, the deployment of technology to contribute or make complex or high-stakes decisions — such as the use of FRT in digital identity — should be examined as a socio-technical system, necessarily involving a combination of technical infrastructure and human involvement.[14]

Applying that approach to this project, being a good provider of digital services relies on more than just state-of-the-art technology solutions. It requires a system-wide approach, with clear legal guardrails, robust governance mechanisms, skilled staff, and placing the human rights of citizens at the centre of design and decision making. This is especially important for government digital service delivery.

Government agencies all around the world often hit one of two major hurdles during the development and rollout of major digital technology projects. One is commencing a project without the relevant skills, expertise or oversight mechanisms to identify and manage the risk of harm. On the other end of the spectrum, some government agencies will accept that they know very little about the technology they are seeking to deploy and defer all control to an external vendor.

Neither of these scenarios allows for robust governance, accountability mechanisms or the cultivation of citizen trust in digital government service delivery.

Throughout this project, Service NSW has adopted a considered and consultative approach to the implementation of NSW Digital ID. Collaborative discussions with HTI and Service NSW considered multiple aspects of the digital identity system, from community engagement, accessible design, the potential impact on privacy and the need for NSW Digital ID to be grounded in law.

HTI understands Service NSW has also engaged other experts in digital identity, as well as relevant NSW regulators.

The value of early expert consultation

The development and implementation of AI-based technologies by the NSW Government is a critical but complicated policy field to navigate, necessitating input from multiple stakeholders. This is particularly the case given the policy process is interrupted by the parliamentary electoral cycle, as has occurred with the rollout of NSW Digital ID.

Along with establishing strong lines of communication with their responsible Minister, Service NSW and the Department of Customer Service must also build trust and transparency with the identity credentials and face verification vendors they undertake procurement with, as well as engage closely with the expert review process via the NSW AI Review Committee.

Additionally, as demonstrated through this JMI grant project, there is real value in engagement with independent experts like HTI—that is, experts who sit outside of government but can provide disinterested knowledge and advice.

In this environment, each stakeholder has an important role to play in the processes of government accountability and good service delivery. However, these outcomes become both optimised and realised for citizens when there is a symbiosis between all these players, and when these processes become mutually reinforcing.

Lessons for other Australian jurisdictions

As outlined above, there is now a strong national commitment to a coordinated digital identity system across all jurisdictions. In this environment, the NSW Government has an opportunity to lead by example in terms of best practice technology design, policy development and supporting legislation for digital identity.

There is a significant opportunity for other jurisdictions to draw from the tested approach taken by Service NSW, guided in part by the provision of independent expert and regulatory advice.

In particular, the governance framework and training strategy outlined in this document could easily be adopted by other jurisdictions, including the Commonwealth Government, to guide the development of nationally accountable and interoperable digital identity legislation and systems.

The adoption of these important safeguards in other jurisdictions would ensure all Australian citizens enjoy the same level of service delivery relying on digital identity, while the same safeguards for privacy, for example, are in place for all Australian residents. There is much to be learned from the lengthy and in-depth policy process Service NSW has undertaken to date. If the NSW Digital ID rollout continues along its current trajectory, including the tabling of legislation, the NSW Government is in a position to adopt a world-leading, trustworthy and high-quality digital identity system, worthy of adoption and adaptation by other Australian governments.

Endnotes

[1] Minister for Customer Service and Digital Government, “NSW Digital ID set to provide people greater control over their online privacy”, NSW Government, 1 May 2023, https://www.nsw.gov.au/media-releases/privacy-week-nsw-digital-id.

[2] Department of Customer Service (NSW), “NSW Government unveils the 'future of digital identity'', NSW Government, 5 April 2022, https://www.nsw.gov.au/customer-service/media-releases/nsw-government-unveils-future-of-digital-identity.

[3] NSW Government, Choose NSW Digital ID, https://www.nsw.gov.au/nsw-government/projects-and-initiatives/benefits.

[4] James Martin Institute for Public Policy, 2022 Policy Grant Winners, https://jmi.org.au/2022-policy-challenge-grant-winners/#_1.

[5] UK Government, Department for Science, Innovation and Technology, “Guidance: Enabling the use of digital identities in the UK”, 13 February 2023, https://www.gov.uk/guidance/digital-identity.

[6] Australian Government, National Strategy for Identity Resilience (Canberra: Australian Government, 2023), https://www.homeaffairs.gov.au/criminal-justice/files/national-strategy-for-identity-resilience.pdf.

[7] Australian Government, Identity Verification Services Bill 2023 (Cth) and the Identity Verification Services (Consequential Amendments) Bill 2023 (Cth), https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7085.

[8] Australian Government, Digital ID Bill 2023, and the Digital ID (Transitional and Consequential Provisions) Bill 2023, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/DigitalIDBills2023.

[9] Nicholas Davis, Lauren Perry and Edward Santow, Human Technology Institute, Facial recognition technology: Towards a model law (Sydney: UTS, 2022).

[10] NSW Government, “NSW Digital ID will make government more accessible”, 6 June 2023, https://www.nsw.gov.au/nsw-government/projects-and-initiatives/nsw-digital-id/digital-id-journey/nsw-digital-id-will-make-government-more-accessible.

[11] For example, see Amazon Web Services, What is facial recognition, https://aws.amazon.com/what-is/facial-recognition/#:~:text=Banking,passwords%20for%20hackers%20to%20compromise.

[12] NSW Government, “Putting you in control of your identity, https://www.nsw.gov.au/nsw-government/projects-and-initiatives/nsw-digital-id.

[13] Nicholas Davis, Lauren Perry and Edward Santow, Human Technology Institute, Facial recognition technology: Towards a model law (Sydney: UTS, 2022), 16.

[14] Eric Trist, “On socio-technical systems”, Sociotechnical Systems: A sourcebook, William A. Pasmore (ed.), (Ann Arbor: University Associates, 1978), 43; Fred Emery, “Characteristics of Socio-Technical Systems”, The Social Engagement of Social Science, a Tavistock Anthology, Vol. 2, Eric Trist (ed.) (Philadelphia: University of Philadelphia Press, 1993), 157.

APPI

Australian Public Policy Institute

Transforming public policy

Level 1, 60 Martin Place
Sydney, NSW 2000 Australia

E info@appi.org.au | **W** appi.org.au