2 October 2023

Legal and Constitutional Affairs Legislation Committee,
The Senate, Parliament of Australia
By webform:
https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/IDVerificationBills23

AND

Department of Finance
By webform: https://www.digitalidentity.gov.au/have-your-say/2023-digital-id-bill-and-rules-submissions

Digital identity and identity verification bills

About us

The **UNSW Allens Hub for Technology, Law and Innovation** ('UNSW Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law and Justice, the Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the UNSW Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

About this Submission

We are grateful for the opportunity to make submissions as part of the Digital Identity consultation process as well as the more specific invitation we received to make submissions on the related *Identity Verification Services Bill 2023* and the *Identity Verification Services (Consequential Amendments) Bill 2023*. While these have different deadlines, they are all related and thus we have combined our response into a single submission for the earlier date (2 October 2023). In particular, together, this set of legislation establishes a framework for introducing and regulating digital identity in Australia and the operation of identity verification services and provide privacy and security protections for those using them. Our submission reflects our views as researchers; they are not an institutional position. This submission can be made public.

While the subject matter of the legislative framework is substantial, we hope to provide some specific suggestions on three key issues that concern the legislative framework on digital identity systems (DI systems) as a whole.

1. The primacy of biometric technology and its consequences.

2. The bundling of multiple technologies and technological systems within modern digital identity systems and its consequences on privacy and digital rights.
3. Voluntary co-option into the digital identity system and safeguards against mission creep.

Our recommendations, in summary, are:

a. The primacy of biometric technology needs to be questioned before it is adopted wholesale into the digital identity system. Further, specific studies must be commissioned before its adoption into the digital identity system to interrogate bias, accuracy, and the impact on vulnerable categories of people.

b. The *Identity Verification Services Bill 2023* (*"IVS Bill 2023")* and the *Digital Identity Bill 2023* must redline detailed provisions attuned to the specific problems of facial recognition technology (FRT), particularly in its use on indigenous populations, beyond the safeguards in the Privacy Act 1988. Further, we advise a closer study of the multiple technologies that compose DI systems – FRT, automated decision-making processes, and biometrics to understand how best to regulate them effectively.

c. The law must provide additional future-proof safeguards around actual practices surrounding the national DI system, voluntary or otherwise, to protect against any mission creep.

Each of these has been discussed in more detail, and the rationale for our recommendations is provided below.

Primacy of Biometric Technology and Its Impact

The use of biometric technology to verify identities and build a holistic digital identity system in Australia is evident in the proposed bills. This submission advises against an approach favouring biometrics as the primary authentication technology. Principally, biometric identification rests on the premise that the biometric measurements given by the body are scientific, infallible, and more reliable than human self-identification. It privileges machine-readable information over human assertion of identity, despite reported errors of registration, technical glitches with authentication, and biases noted with verification technologies. Various academics and civil society activists have also advanced this argument in the previous consultative round on the *Digital Identity Bill 2019*. There are multiple reasons for reconsidering biometric technology as the primary authentication method of identity.

First, biometric technology's promise of accurate verification remains largely unverified and untested. Despite claims of infallibility, evidence worldwide has shown the limited theoretical work conducted in this field, specifically to interrogate the notions of bias and fairness, instead relying on simpler statistical definitions of group fairness and error rate parity, which the legislative framework also reiterates. Even those advocating widespread biometric use and adoption argue that biometrics for authentications are still relatively new and necessitate further study. Researchers have documented the various parameters which affect the performance of biometric technologies and technologies underpinning them like fingerprint systems. These include demographical factors – age, ethnicity, and people subject to skin transformations; user's anatomies that are different from when they were enrolled – beards, moustaches, baldness; environmental conditions – humidity and temperature; and capture systems – quality variations of different sensors, affecting the accuracy of biometrics. The Digital ID Accreditation Rules 2024 attempt to control for these issues by specifying the testing of biometric matching algorithms as per established standards like ISO/IEC 19795-2 and

ISO/IEC 19795 – 9. However, these standards are formulated for testing biometric systems under monitored and not controlled conditions; and the used dataset is mainly heterogeneous, which does not allow for the isolation of particular situations as the rest of the test population 'smoothes over these cases'. Studies have also found mismatches between the stakeholders' interests and what has been prescribed in standards and guidelines that apply to biometric performance testing. Further, many of these standards only acknowledge traditional methodologies of forgeries and do not sufficiently account for new technologies of cyber offences, including deepfakes.

Second, biometric technologies have the capacity to exclude people who fail to be verified by them. They have the potential to negatively impact older populations more directly due to ageing affecting bodily functions like touch, imaging, speech, and body language. As mentioned above, biometrics involving fingerprints can particularly affect older people, manual workers, and those affected by diseases that impact the skin, impacting the accuracy of recognition, or even exclusion from services if those services are contingent on biometric authentication. This has been prominently demonstrated in countries which have adopted large-scale biometric technology. In India, which has implemented the world's largest biometric digital identity program, poorly planned and implemented systems have severely affected human rights, and for both technological and sociological reasons, have ended up excluding and disenfranchising almost two million people. Similarly, in the Dominican Republic, the national digital ID system fuelled the retroactive exclusion of people of Haitian descent from the civil registry.

Third, biometric information largely consists of sensitive information, which may require special protection against data breaches. This has also been recognised both in these draft legislations and in the *Privacy Act 1988*. As such, any breach of data, fraud, or any other cyber-security incident which discloses the biometric information of people may have far more serious consequences than a breach of personal information. In this context, the use of automated services for the disclosure of sensitive information could pose several challenges, particularly in light of the *IVS Bill 2023* seeking to amend the *Australian Passports Act 2005* to allow for automated disclosures of personal information to a specified person via the document verification service or the face verification service. It must also be noted that the *IVS Bill 2023* and the *Digital Identity Bill 2023*, along with the *Privacy Act 1988* rely on a consent and at times, express consent regime. The challenges of relying on such a regime without specifying the requirements for express consent have been detailed in our previous submission in 2021. We note the proposal to reform the *Privacy Act 1988* in this regard.

Fourth, the ability of biometric identification to detect frauds and cyber security threats is contingent on design of the system as a whole. Ultimately, biometric data is converted into digital information, which leaves open the possibility of "man in the middle" attacks.

Biometric identification services exacerbate conditions of discrimination, social inequalities, and violation of human dignity, to the detriment of disadvantaged and less digitally educated segments of the population. Therefore, we advise against favouring biometrics as the primary authentication method in a digital identity system. Further, specific studies must be commissioned before its adoption into the digital identity system to examine the impact of biometric technologies, particularly interrogating bias, accuracy, and its impact on vulnerable categories of people.

Bundling of Multiple Technologies and Systems Within Modern Digital Identity Systems and its Consequences on Privacy and Digital Rights

Modern DI systems combine features of older identification systems with modern biometrics and other digital technologies. Digital identity is placed at this interplay of complex relationships between technology, identification, and identity, interacting with biometric data and governmentissued identity documents. DI systems, therefore, encapsulate various actors – both public and private sector operating on different motivations, and technologies. These technologies have been broadly classified into biometric technology, authentication technologies such as blockchain, and predictive analytics that build on technologies linked to data analytics. Both the *IVS Bill 2023* and the *Digital Identity Bill 2023* create an elaborate framework of digital identification verification technologies, that combine multiple technologies including but not limited to facial recognition, database management, authentication software, and biometric matching algorithm. The regulation of DI systems therefore must encompass questions of regulation of multiple technologies bundled together.

Apart from the challenges in using and regulating biometric technology discussed in the earlier section, FRT as one of these bundled technologies poses one of the greatest challenges in regulating digital identity. Researchers have shown that facial recognition technology is intertwined with other social and political recognition types. This means that despite efforts to 'diversify' and 'debias' facial recognition, it may exacerbate the discriminatory effects it seeks to resolve and make identity verification unreliable. The *IVS Bill 2023* allows for facial recognition or facial identification services to be used for both 1:1 matching service and 1: many matching services. This is concerning for multiple reasons.

First, FRT highlights the nebulous connection between identity and appearance. Since FRT relies on computer vision, where recognition is always a one-sided visual assessment, there is a danger of misreading or misrecognising a person's identity. This misrecognition and mislabelling by technology can often counter a person's self-identity, especially when it relates to a person's gender identity or race. FRT has been criticised, particularly in its use by law enforcement agencies, for being violative of civil liberties, and for the potential for abuse, propensity for inaccuracies, and improper use.

Second, technical studies on using such technology on indigenous people in Australia who may be particularly vulnerable and impacted disproportionately by misrecognition and misidentification have not been exhaustively conducted. A few studies conducted on FRT technology in Australia have identified FRT's inaccuracies in recognising non-white faces and being of particular threat to Indigenous Australians. This is concomitant with studies conducted in the United States which have shown FRT to have a disparate impact on communities of colour.

Therefore, we recommend that both bills redline detailed provisions attuned to the specific problems of FRT, particularly in its use on indigenous populations, beyond the safeguards given in the *Privacy Act 1988*, which may not be sufficient to guard against misuse and mass surveillance. These concerns were mirrored in the Advisory report on *the Identity-matching Services Bill 2019* and the *Australian Passports Amendment (Identity-matching Services) Bill 2019*. Further, we advise a closer study of the multiple technologies that compose DI systems – FRT, automated decision-making processes, and biometrics to understand how best to regulate them effectively.

Voluntary Co-option into the Digital Identity System and Safeguards on Eventual Mission Creep

The *Digital Identity Bill 2023* purports to keep the system voluntary for users. This is reflected in clause 71(1) of the *Digital Identity Bill 2023*, which states that a participating relying party must not require an individual to create or use a digital identity as a condition of providing a service or access to a service. However, sub-clause (1) does not apply to a service that provides access to another service; and an individual can access the other service without creating or using a digital identity through the Australian Government Digital ID System. However, the availability of alternatives does not create a system where service providers can be precluded from offering digital identity as the more convenient and cheaper option. Further, sub-clause (4) states that the Digital ID Regulator may grant an exemption to a participating relying party if satisfied that it is appropriate to do so. While the provision has safeguards against arbitrary grant of exemptions, a creeping expansion of businesses that superficially satisfy the prescriptive requirements of the law may lead to a slow expansion of the exemption clause. This can, over time, create an ecosystem where despite claims of voluntariness, digital identity becomes both the de facto and de jure DI system, creating anxieties of recognition and sometimes exclusion of people. This has been witnessed in other countries that also started the national digital identity program purely voluntarily.

In India, where the national digital identity project (Aadhaar) began in 2009 as ‘voluntary’, soon witnessed public-sector oil marketing companies and financial institutions including banks and fintech providers beginning to heavily rely on it for e-KYC authentication, expanding eventually to income tax filing, transfer of government subsidies, mobile phone connections, and government scholarships and welfare programs. Today, despite legislative safeguards and a subsequent Supreme Court of India decision in 2018, the in-practice voluntary feature of Aadhaar remains disputed. The Indian example of the conversion of Aadhaar from a voluntary DI system to the only identification system has raised serious questions about civil liberties and democratic practices, mirrored in other countries including China, Kenya, and Jamaica. Its linkage to expansive fintech operations including banking, payments, and welfare services has also led to the creation of financial surveillance infrastructures detailed in academic studies.

In the Australian context, the other unintended consequences of the voluntary feature and people not having a real choice have been detailed in our previous submission. These concerns have also been raised in the *Identity–Matching Services Bill 2018/2019*, and have been linked to the growth of a ‘creeping surveillance state’. Further, concerns around the inadequacy of the 2017 Intergovernmental Agreement on Identity Matching Services, referenced in the *IVS Bill 2023* and its effect on the centralisation of identity databases and the legal concentration of power have also been well documented and must be acknowledged for the present legislative framework under discussion.

As such, we would recommend additional future-proof safeguards around actual practices surrounding the national digital identity system, voluntary or otherwise, and to protect against any mission creep.

Yours sincerely,

Shohini Sengupta