6 November 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

Identity Verification Bills 2023

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 respond to a question we took on notice while giving evidence for the Committee on 30 October 2023. This submission is in addition to the submission made on 2 October 2023 to the Committee on the *Identity Verification Services Bill 2023* and the *Identity Verification Services (Consequential Amendments) Bill 2023*. Our submission reflects our views as researchers; they are not an institutional position. This submission can be made public.

The question asked to us by Senator SCARR was about the operation of other legislation and how it may act in a way that denudes the privacy obligations in this act—for example, in instances of national emergency. The Senator made specific reference to the *Biosecurity Act 2015* under which the Minister for Health can make a declaration of national emergency and issue orders and regulations which are not disallowable and which effectively enable him to amend any law. The Senator said that this power to amend any law would include all the privacy protections contained in this legislation.

Analysis

Our analysis of the *Biosecurity Act 2015* reveals that Part 2 of the Act gives the Minister extensive powers to issue directions. Additionally, s 477(2) states that s 42 (disallowance) of the *Legislation Act 2003* does not apply to a biosecurity emergency declaration.

These powers under the *Biosecurity Act 2015* (s 475) were used for the first time on 18 March 2020 in response to the COVID-19 outbreak in Australia when the Governor-General declared that a human biosecurity emergency existed. The declaration gave the Minister for Health expansive powers to issue directions and set requirements to combat the outbreak. In this regard, the Report

of the Senate Standing Committee for Regulations and Ordinances in 2019 reflected the view of the Committee that exempting delegated legislation from disallowance was a serious matter, as this may remove or undermine parliamentary oversight. The Final Report of the Senate Standing Committee for the Scrutiny of Delegated Legislation in 2021 also recommended the Senate Standing Committee for the Scrutiny of Bills or another independent body or person conduct a review of the appropriateness of the delegation of legislative powers in the *Biosecurity Act 2015*, including the appropriateness of provisions which exempt delegated legislation made pursuant to these powers from parliamentary oversight.

We believe that the fundamental issue of excessive delegated legislation, without adequate Parliamentary checks and balances may lead to an eventual mission creep of identification technologies as highlighted in our earlier submission to the Committee. We draw attention to India's Digital identity Program (Aadhaar) which saw a similar creeping expansion, without adequate legal safeguards particularly during the COVID-19 pandemic. In 2020, India introduced a contact tracing app (Aarogya Setu), connecting each individual user with their unique identification number (Aadhaar number) for validation of their data. Although the app was introduced as 'voluntary', it was soon pushed aggressively by multiple State authorities including the Ministry of Home Affairs. Aarogya Setu derived its legality from the *Disaster Management Act 2005* which is a comparable legislation to Australia's *Biosecurity Act 2015*. The *Disaster Management Act 2005* in India allowed the Union Government to lay down guidelines for, or give directions to other State authorities, Ministries and Departments regarding any measures to be taken in light of a disaster. The law also allowed the State to make, or amend any rule, regulation, notification, guideline, instruction, order, scheme or bye-laws for the prevention or mitigation of disasters.

These unchecked powers of the executive without adequate Parliamentary oversight have been criticised by scholars as excessive, violative of the right to privacy and personal autonomy, and amenable to misuse particularly during times of disasters. The contact tracing app itself was claimed to be hacked, revealing people's health status and exact location. While the Indian Government denied the hack, India's digital identity program, inclusive of the many applications of the identification technology, has had several data breaches over the years, exposing millions of citizens to privacy and cybersecurity threats. The latest data breach has been reported from last week as one of the country's largest data breaches so far with the personal details of over 815 million people leaked online.

The other issue with excessive and unchecked delegated power, especially during times of disasters is the convergence of multiple digital technologies of identification that exacerbate conditions of surveillance and data breaches. In the case of India, COVID-19 saw the roll-out of a dozen government applications that used a combination of features, including GPS surveillance, facial recognition and thermal imaging, to identify and trace the potential carriers of the virus, enforce quarantines and lockdowns, and allocate additional healthcare resources. Despite privacy protections, and the collection of aggregated and anonymised data through such digital technologies, the threats of such data being leaked and anonymised information being re-identified nevertheless persist. Scholars have persistently pointed out how Aarogya Setu violated the proportionality principle through expansive provisions giving the executive wide powers, lacked a sunset clause, and facilitated excessive collection, processing, storage, and sharing of sensitive personal data with an increasing number of State authorities. This poses concerns for both cybersecurity and surveillance.

Similar challenges of disaster management or biosecurity laws allowing for digital technologies without adequate safeguards has also been seen in other countries. For instance, in Singapore, the Ministry of Home Affairs confirmed that personal data collected during the pandemic using

identification and contact tracing technologies were being used by the police for criminal investigations. This is despite assurances made during the pandemic to people that personal data collected during the pandemic would only be used in a limited fashion during the pandemic. Police in Australia also sought to use QR code check-in data, and WA Police did so twice without a warrant. Similar concerns were also raised for the UK's proposals of digital immunity passports combining biometric digital identity with contact tracing technologies. Scholars have warned that these technologies pose risks to human rights resulting from surveillance, and additional risks due to uneven distribution of surveillance on certain communities and people, magnifying existing inequalities, inaccuracies, and trust deficiencies.

Our Recommendation

As such, we advise caution and careful consideration of the impacts of other legislation such as the *Biosecurity Act 2005* on privacy and the IVS Bill. This is because certain provisions of the *Biosecurity Act 2005* may lay the foundations for indiscriminate use of digital identification technologies, in combination with other technologies, particularly in times of national disasters. As has been seen in the context of COVID, this can lead to legitimate cybersecurity and surveillance concerns. There is a need for adequate legislative safeguards around actual practices surrounding the national digital identity system, voluntary or otherwise, and to protect against any future mission creep.

Following on from our oral testimony, we suggest that further consideration be given to amending the Bills either before they are passed or, if that is not possible due to urgency, then after a sunset period that would enable full consideration alongside the digital identity system as a whole and the *Privacy Act 1988* reforms.

Yours sincerely,

Lyria Bennett Moses and Shohini Sengupta