23 February 2024

Senate Economics Legislation Committee,
The Senate, Parliament of Australia
By webform:
https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/DigitalIDBills2023

Digital ID Bill 2023 & Digital ID (Transitional and Consequential Provisions) Bill 2023
Question on Notice

Question on Notice

We are grateful for the opportunity to respond to a question we took on notice while giving evidence for the Committee on 9 February 2024. This response is in addition to the submission made on 17 January 2024 to the Committee as part of the consultation process for the Digital ID Bill 2023 & Digital ID (Transitional and Consequential Provisions) Bill 2023. Like our submission, it reflects our views as researchers.

The question asked to us by Senator Shoebridge was how to ensure that the police and the security apparatus was precluded from having any means of gaining access to sensitive data acquired under this legislation. The Senator made specific reference to India and asked us to provide more information in this regard.

Analysis

I. Australia

In our view, the Digital ID Bill 2023 & Digital ID (Transitional and Consequential Provisions) Bill 2023 does not include sufficient safeguards to preclude national security and law enforcement agency access. Any substantive reform on surveillance, privacy protections and instituting legislative safeguards will require several amendments to multiple laws, and legislative frameworks on policing, security, and emerging technologies. However, in this submission, we have focussed on a few examples from both Australia and the Digital ID Bill 2023 under consideration, as well as India to emphasise systemic challenges that pervade the Digital ID infrastructure as a whole.

In particular, we would like to draw attention to section 54 of the Digital ID Bill 2023. The provision states that 'Certain personal information must not be used or disclosed for prohibited enforcement purposes.' However, there are six categories of exceptions in s 54(1). In addition, section 54(2) provides that the restriction on the disclosure of personal information does not apply in relation to enforcement related activities conducted by, or on behalf of, an enforcement body under, or for the purpose of, the Digital ID Bill or the Privacy Act 1988. These enforcement bodies, as per section 6(1) of the Privacy Act, 1988, can include the Australian Federal Police, a police force or service of a State or a Territory, regulatory bodies, prescribed authorities and bodies established under the law of a State or Territory to conduct criminal investigations or inquiries. Further, enforcement related activities under the same provision can include the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of certain laws, and the conduct of surveillance activities, intelligence gathering activities or monitoring activities. Further, 2021 amendments to the

Surveillance Devices Act 2004, the *Telecommunications (Interception and Access) Act 1979* and the *Crimes Act 1914* strengthened existing law enforcement surveillance powers. In particular, they introduced new powers to collect intelligence on serious criminal activity by permitting access to the devices and networks used to facilitate criminal activity.

In this regard, we draw particular attention to the Australian Human Rights Commission's Human Rights and Technology Final Report (the Report) released in 2021, which advised that responsible innovation must be accompanied with human rights measures to foster a 'firm foundation of public trust in new and emerging technologies that are used in Australia.' In particular, the Report recommended that federal, state and territory governments should introduce legislation for the regulation of facial recognition and biometric technology to expressly protect human rights, and 'apply to the use of this technology in decision making that has a legal, or similarly significant, effect for individuals, or where there is a high risk to human rights, such as in policing and law enforcement.'

II. India

In India, where the Digital ID infrastructure (called 'Aadhaar') has been in operation for the past two decades, there has been an alarming rise in policing and surveillance revelations by law enforcement to target human rights activists. Last year, it was reported that, despite a Supreme Court ruling that metadata not be stored by the Digital ID regulator and authenticating entities beyond six months, several state level police departments across India were using metadata for the collection and tracking of information, surveillance of network activity and other law enforcement activities at both the Union and state level.

An independent study on the 'Status of policing in India Report 2023' noted that digital surveillance had expanded the powers of states to surveil and collaborate with private actors with even greater capacities to grab mass data. For instance, in 2015, the state of Delhi launched the Crime Mapping, Analytics and Predictive Systems (CMAPS) for live spatial hotspot mapping of crimes, criminal behaviour patterns, and suspect analysis. Efforts to acquire information regarding both CMAPS' usage and efficiency have been unfruitful because of the large exceptions for law enforcement provided under India's *Right to Information Act 2005*. The Report also noted that police surveillance was also more likely to be directed against socio-economically vulnerable groups such as Dalits, Adivasis, and religious minorities. There would be similar risks in Australia to for indigenous and other at-risk communities. In early April 2022, the Indian Parliament also passed the *Criminal Procedure (Identification) Act 2022* which authorised executive authorities, including the police and prisons departments, to collect, analyse and store biometric and personal data on any person who has been arrested, including both undertrials or convicts. This raises privacy concerns particularly given that in India (as in Australia) people should be presumed innocent until proven guilty. Concerns have also been raised about the fact that CMAPS may even be used to collect the personal information of those apprehended under the various preventive detention laws, thus widening the surveillance net further. Surveillance concerns are exacerbated by data breach concerns. For instance, cybersecurity experts earlier last year pointed out that Aadhaar numbers, along with other sensitive data for over a billion people, were available on the internet for sale for less than $10.

Our Recommendation

As such, while we appreciate that the Digital ID bill seeks to narrow the scope of disclosure to law enforcement, we caution that repurposing of the Digital ID architecture for surveillance and security related purposes poses risks. This has also been reiterated by other civil society organisations in previous consultations over the Digital ID Bill. As has been seen in India, sharing with law enforcement generates cyber security and surveillance concerns, particularly given reduced

transparency relating to law enforcement practices. Hence, we urge greater legislative restrictions on national security and law enforcement use of the national digital identity system, voluntary or otherwise. We also caution more generally against future mission creep.

Yours sincerely,

Shohini Sengupta and Lyria Bennett Moses