Canberra Declaration
1A–227 Cordeaux Road
Mount Kembla NSW 2526
+612 4272 9100
info@canberradeclaration.org.au

Senate Standing Committees on Economics
Phone: +61 2 6277 3540
economics.sen@aph.gov.au

Digital ID Bill 2023

19 January 2024

Co-Authors

Warwick Marsh, Co-Founder, Canberra Declaration

Alison Marsh, Co-Founder, Canberra Declaration

Samuel Hartwich, Research Consultant, Canberra Declaration

Kurt Mahlburg, Research and Features Editor, Canberra Declaration

Jean Seah, Managing Editor, The Daily Declaration

Kym Farnik, Prayer Coordinator, Canberra Declaration

Table of Contents

1.0 Executive Summary

Representing our over 92,000 signatories, the Canberra Declaration is a grassroots network of caring Australians committed to the preservation of faith, family, freedom and life. We affirm the legal reality, etched into the preamble of the Constitution, that Australians are a people "humbly relying on the blessing of Almighty God". We believe that God's blessing will endure in our nation to the extent that we continue to humbly rely on Him. Our vision is to see our country's Judeo-Christian values revitalised for the good of all Australians. We welcome the opportunity to present our submission to this Inquiry.

While we can see some pragmatic reasons for the proposed digital identity system to be set up in Australia (and others have put forth that case), we are gravely concerned about the consequences the passage of these bills will have on the privacy and freedom of Australia's citizens. Consequently, we stand in opposition to these bills.

In this submission, we will put forth the case that the Digital ID Bill 2023 as it currently stands must be rejected. Digital ID poses a grave risk to the privacy and freedom of the individual. By centralising information into a single database, with the ability of digital ID to be used for an ever-expanding list of uses, it places too much power and control in the hands of the government.

A centralised system creates a security issue as it becomes the single target for hackers and identity thieves. In addition, there are good reasons to seriously doubt the practical ability to maintain digital ID as purely voluntary. The case study of India's Aadhaar system brings these concerns out into the open and provides a real-world look into the problematic nature of a centralised digital ID system.

In short, we agree that while "protecting our digital identities is a welcome and well-overdue part of this proposed bill, getting it wrong could lead to harm at an even larger scale."[1]

Therefore, we reject this bill as it stands. Thank you for taking the time to review our submission.

[1] Erica Mealy, "A national digital ID scheme is being proposed. An expert weighs the pros and (many more) cons", *The Conversation*, 26 September 2023, <https://theconversation.com/a-national-digital-id-scheme-is-being-proposed-an-expert-weighs-the-pros-and-many-more-cons-214144>.

2.0 Lack of Consultation

The Digital ID Bill 2023 Explanatory Memorandum correctly states that "Digital ID is a major economy-wide reform".[2] Considering the significant and major change the bill seeks to implement, it is difficult to understand the limited amount of time that has been given for public consultation.[3]

Only three weeks (from 19 September–10 October 2023) were set aside during the initial consultation period into digital ID.[4] This was an "extremely short consultation period"[5] considering the scope of the changes currently under consideration.

These two bills were given to the Senate Standing Committees on Economics for inquiry and report on 30 November 2023 just before the busy Christmas and New Year periods. With the deadline for submissions closing on 19 January, this small window of opportunity for public consultation "doesn't provide much confidence a fit-for-purpose solution [i.e. a safe digital ID system] will be created".[6] Sadly we believe the government intends to push this legislation through with as little scrutiny as possible.

3.0 Safety and Security

3.1 A Central Point of Failure

The Digital ID Bill 2023 aims to set up a system that will collate all our personal data into one system. One obvious drawback of such as scheme is that it creates "a single point of failure".[7] This "single point of failure for both privacy and authentication" will result "in an extremely brittle architecture that would allow for large-scale identity fraud if that one component came under the control of a malicious party."[8]

---

[2] Digital ID Bill 2023 Explanatory Memorandum, <https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/s1404_ems_e64ce90b-5f6c-4ad9-aad3-51d0a97bc4fc/upload_pdf/EM_JC011670.pdf;fileType=application%2Fpdf>, page 3.
[3] Gary Christian, "The haunting certainties of Australian Digital ID", *Spectator Australia*, 3 January 2024, <https://www.spectator.com.au/2024/01/the-haunting-certainties-of-australian-digital-id/>.
[4] https://www.digitalidentity.gov.au/have-your-say.
[5] Erica Mealy, "A national digital ID scheme is being proposed. An expert weighs the pros and (many more) cons", *The Conversation*, 26 September 2023, <https://theconversation.com/a-national-digital-id-scheme-is-being-proposed-an-expert-weighs-the-pros-and-many-more-cons-214144>.
[6] Ibid.
[7] Ibid.
[8] Ben Frengley and Vanessa Teague, "Submission to the Consultation on Digital ID", January 2023, <https://www.digitalidentity.gov.au/sites/default/files/2021-01/consultation01-vanessa-teague.pdf>: 2.

By placing all our data in one place, it creates a lucrative opportunity for hackers. When, not if (we consider data breaches inevitable at some point) hackers break through, they will have access to a broad range of sensitive information. Considering digital ID will include facial recognition and other biometric data, this poses a severe risk of identity theft.

While it is true that our security measures continue to advance, it is nevertheless the case that so do the criminal methods to break into those systems. There is simply no guarantee in any system.

In addition, smartphones would be the common method of using digital ID verification through apps such as MyGov. This means that even if the government were 100% successful in implementing an impenetrable digital ID database system on their end, "the proposed scheme would still only be as secure as your phone. Having a weak password, losing your phone, or having your phone hacked could lead to data being compromised."[9]

3.2 Recent Examples of Cyber Attacks

Cyber attacks and data breaches are now, tragically and concerningly, commonplace. Some recent examples include Optus in October 2022, Medibank in November 2022, the NSW Government in April last year, and the prime minister's office, the Reserve Bank of Australia and Australia Post as recently as 14 January 2024.[10] Whether government agencies or private companies, organisations have been wholly unable to prevent data leakage to internet thieves.

The federal government has a poor track record of securely storing data. Considering it would oversee a centralised digital ID system, this history does not inspire confidence in the proposed digital ID system.

In July 2023 *ABC News* revealed that fraudsters were able to exploit a security loophole to gain access to ATO records through false myGov accounts.[11] Astonishingly, the fraud cost taxpayers half a billion dollars over two years. Of high concern is that it took two years to

---

[9] Erica Mealy, "A national digital ID scheme is being proposed".
[10] "Albanese government loses national security information in data hack", *Sky News*, 14 January 2024, <https://www.skynews.com.au/australia-news/politics/albanese-government-loses-national-security-information-in-data-hack/video/5c0b807f45b7fd2c2e828978a9fb9e07>.
[11] Sarah Curnow, Dan Oakes and Kevin Nguyen, "ATO reveals more than $557 million claimed by fraudsters exploiting security loophole", *ABC News*, 26 July 2023, <https://www.abc.net.au/news/2023-07-26/ato-reveals-cost-of-mygov-tax-identity-crime-fraud/102632572>.

uncover the fraud.[12] Since the government was unable to prevent criminals from exploiting a loophole in the current digital identity system, it is impossible to understand how a new piece of legislation will come up with an impenetrable solution.[13]

We agree with the statement that the government has an "appalling track record of protecting such information, from wholesale breaches of Census data to the My Health Record hacks and infiltration of the Australian Driver Licence database, and of course the systematic misuse of metadata accessed through its compulsory metadata retention scheme."[14]

In short, placing a centralised ID system, including sensitive biometric data, at the responsibility of the government is cause for great concern.

3.3 Case Study: India's Aadhaar System

Begun in 2009, India's Aadhaar programme is a 12-digit unique-identity number that involves collecting the individual's fingerprints, retinal scans and facial photos.[15] Aadhaar makes an ideal case study since it is the world's largest biometric ID system with over 1.3 billion enrolments.[16]

Consequently, it is not surprising that the World Economic Forum (WEF), in its 2016 publication "A Blueprint for Digital Identity", pointed to India's Aadhaar program as an example of the benefits of digital ID.[17] Yet even at this time, that same publication noted that while the "Aadhaar program has been very effective in increasing financial inclusion with over 1 billion people enrolled for accounts", the report records "some outstanding concerns about information protection and privacy."[18]

---

[12] Sonia Hickey, "Fraud Enabled by MyGov 'Security Gap' Costs Australian Taxpayers $500 Million", Sydney Criminal Lawyers, 29 July 2023, <https://www.sydneycriminallawyers.com.au/blog/fraud-enabled-by-mygov-security-gap-costs-australian-taxpayers-500-million/>.
[13] Richard Chirgwin, "ATO attackers filed $557 million in false claims", *itnews.com.au*, 26 July 2023, <https://www.itnews.com.au/news/ato-attackers-filed-557-million-in-false-claims-598448>.
[14] Sonia Hickey, "Fraud Enabled by MyGov 'Security Gap' Costs Australian Taxpayers $500 Million", Sydney Criminal Lawyers, 29 July 2023, <https://www.sydneycriminallawyers.com.au/blog/fraud-enabled-by-mygov-security-gap-costs-australian-taxpayers-500-million/>.
[15] Mardav Jain, "The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment", University of Washington News, 9 May 2019, <https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment>.
[16] Aadhaar Dashboard, Unique Identification Authority of India, Government of India, <https://uidai.gov.in/aadhaar_dashboard/index.php>, accessed January 2024.
[17] WEF, "A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity", Future of Financial Services Series, <https://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf>, August 2016: 86.
[18] Ibid.

Aadhaar has been plagued with problems since its inception. Concerningly, the Aadhaar system has been at the centre of multiple data leaks. In 2017 over 200 official government websites accidentally made Aadhaar data public on the internet.[19] Multiple cyber attacks occurred in 2018 which potentially compromised all the records of all 1.1 billion users.[20] In January of that year, the BBC reported that criminals were selling access to Aadhaar at a rate of 500 rupees for 10 minutes.[21] A further data breach in March involving the state-owned utility company, Indane, allowed access to private information on all Aadhaar users.[22]

One humorous but unfortunate example involves the then Telecom Regulatory Authority of India (TRAI) chairman Ram Sewak Sharma. In an attempt to prove the safety of the Aadhaar system, Sharma tweeted his Aadhaar number in a defiant stunt in 2018.[23] In response, Twitter users were able to obtain the chairman's physical and email addresses, date of birth, and mobile and frequent flyer numbers. Someone even reportedly ordered him a new phone via Amazon, with cash payment required on delivery.[24]

When Aadhaar was released, it was presented as a voluntary scheme. The voluntary nature of Aadhaar was declared by the Supreme Court in September 2013 when the court ruled that no citizen was to be denied access to services in the absence of holding the card.[25]

However, the Government of India increasingly moved to make the system essential for an increasing number of financial activities. From 2016 the government made holding an Aadhaar number necessary for filing a tax return, opening a bank account, obtaining a loan and buying and selling property.[26] In addition, several banks were refusing to take on new

---

[19] Tech2 News Staff, "Aadhaar security breaches: Here are the major untoward incidents that have happened with Aadhaar and what was actually affected", *Firstpost*, 25 September 2018, < https://www.firstpost.com/tech/news-analysis/aadhaar-security-breaches-here-are-the-major-untoward-incidents-that-have-happened-with-aadhaar-and-what-was-actually-affected-4300349.html

[20] WEF, "The Global Risks Report 2019: 14th Edition", 2019, <https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf>.

[21] "Aadhaar: 'Leak' in World's Biggest Database Worries Indians", *BBC News*, 5 January 2018, <https://www.bbc. com/news/world-asia-india-42575443>.

[22] Zack Whittaker, "A new data leak hits Aadhaar, India's national ID database", *ZDNET*, 23 March 2018, <https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/>.

[23] Nikhil Pahwa, "By Revealing His Aadhaar Number, the TRAI Chairman Has Opened a Can of Worms", *The Wire*, 30 July 2018, <https://thewire.in/tech/trai-rs-sharma-aadhaar>.

[24] Ibid.

[25] J. Venkatesan, "Don't tie up benefits to Aadhaar, court tells Centre", *The Hindu*, 24 September 2013, updated 2 June 2016, <https://www.thehindu.com/todays-paper/tp-national/dont-tie-up-benefits-to-aadhaar-court-tells-centre/article5162837.ece>.

[26] Geeta Pandey, "Indian Supreme Court in landmark ruling on privacy", *BBC News*, 24 August 2017, <https://www.bbc.com/news/world-asia-india-41033954>.

customers unless they possessed an Aadhaar. Many businesses including phone operators pushed people to obtain one, “at times even arm-twisting citizens to sign up for an Aadhaar number”.[27] Even government schools in New Delhi were reported requiring children to have an Aadhaar to be enrolled in school.[28] Most concerning of all are reports of people starving to death after their rations from the Public Distribution System shops were denied. Their ration cards were cancelled as a result of failing to link them to Aadhaar.[29]

A challenge over the right of the government and businesses to require an Aadhaar number was subsequently held in the Supreme Court. The lawyers representing the government argued for the right to make Aadhaar mandatory (and therefore to collect biometric data such as retina, face and fingerprint scans). The basis of this was that Indian citizens did not have absolute rights over their bodies and that privacy was not an inalienable fundamental right. However, on 24 August 2017, the panel of nine judges decided against the government and ruled that the right to privacy of India’s citizens was constitutional.[30]

India’s Aadhaar system provides an excellent case study for multiple reasons. It demonstrates that a voluntary system can easily transform towards a mandatory one, at both the hands of government and private businesses. And that if enabled, governments can place efficiency over privacy and deny the fundamental rights of their citizens in the process. We do well to learn these lessons.

4.0 Privacy, Security and Freedom of the Individual

4.1 Officially Voluntary but Practically Mandatory?

Section 74 of the Digital ID Bill states “Creating and using a digital ID is voluntary”. While this is welcome, we question the ability to have this robustly maintained. Currently, those engaging with federal government services like Centrelink are heavily dependent on having a MyGovID.[31] Since the new digital ID aims to replace current systems, it is difficult to see how real and practical choices will be maintained for those who do not wish to take up the

---

[27] Ananya Bhattacharya and Nupur Anand, “Aadhaar is voluntary—but millions of Indians are already trapped”, *Quartz*, 26 September 2018, <https://qz.com/india/1351263/supreme-court-verdict-how-indias-aadhaar-id-became-mandatory>.
[28] Ibid.
[29] Amarnath Tewary, “Jharkhand, where not having Aadhaar could starve you to death”, *The Hindu*, 9 June 2018, <https://www.thehindu.com/news/national/other-states/jharkhand-where-not-having-aadhaar-could-starve-you-to-death/article61827611.ece>.
[30] Pandey, “Indian Supreme Court in landmark ruling on privacy”.
[31] Gary Christian, “The haunting certainties of Australian Digital ID”, *Spectator Australia*, 3 January 2024, <https://www.spectator.com.au/2024/01/the-haunting-certainties-of-australian-digital-id/>.

new technology. This concern about the lack of real choice and the practical requirement for individuals to have a digital ID has been noted by many others.[32]

This difficulty is exacerbated for those living in regional and remote areas. If an alternate choice to using the digital ID system requires in-person presence at Services Australia centres, bank branches, etc., the inhibitions due to distance of travel make obtaining a digital ID essential and therefore mandatory in reality and practice.

Further, the government is aiming to reassure the public of the voluntary nature of a new proposal on the back of the COVID-19 pandemic. But during this time, governments stated that COVID-19 vaccines were voluntary, not mandatory. However, many millions of Australians were forced to choose between meaningful participation in society (e.g. keeping their job) or being shut out. It is difficult to believe official lines of informed consent when this very thing was conspicuously absent during the pandemic years.

4.2 Central Bank Digital Currency

Digital ID lays the foundation for other systems to be added in the future, such as a central bank digital currency (CBDC). A CBDC can be programmable, allowing a party in a transaction to control how the money is spent. The UK's *Daily Telegraph*, reporting on an interview with Tom Mutton (a director at the Bank of England) stated,

> "A digital currency could make payments faster, cheaper and safer, but also opens up new technological possibilities, including programming: effectively allowing a party in a transaction, such as the state or an employer, to control how the money is spent by the recipient."[33]

The article correctly states that "Digital cash could be programmed to ensure it is only spent on essentials, or goods which an employer or Government deems to be sensible".[34] This level of control, completely absent from physical cash, is of grave concern to all liberal democracies such as Australia.

---

[32] E.g. see the ACT Human Rights Commission submission at <https://www.digitalidentity.gov.au/sites/default/files/2023-11/act_human_rights_commission_redacted.pdf>.
[33] Tim Wallace, "Bank of England tells ministers to intervene on digital currency 'programming'", *The Telegraph*, 21 June 2021, <https://www.telegraph.co.uk/business/2021/06/21/bank-england-tells-ministers-intervene-digital-currency-programming>.
[34] Ibid.

The programmable nature of CBDC, along with social credit systems like China's, can create a future with heavy government control and surveillance of its citizens. An objection here will no doubt be raised that these topics are outside the scope of the Digital ID Bill 2023.[35] That is true. However, it would seem short-sighted to avoid the larger, difficult ethical and social questions technologies such as CBDC raise.

The central point here is that digital ID is an essential piece of infrastructure that makes CBDC possible.[36] Considering organisations such as the World Economic Forum are consistently pushing to transform the world's digital landscape through digital ID and CBDC, ignoring the larger issues appears a severely blinkered response.[37]

4.3 Canadian Government Abuse of Digital Banking

Here we raise the actions of the Canadian government under Prime Minister Justin Trudeau. The purpose is to demonstrate the exact concerns above of how digital ID could be misused with concrete examples of how a government and banks can combine to violate the rights of innocent citizens. The idea of governments working with banks to control how (or if) people are allowed to access their money is not a fantasy.

Even without digital ID, in 2022 the Canadian Prime Minister froze the accounts of the 'Canadian truckers' who opposed the government's extreme and unscientific vaccine mandates. In February 2022 Trudeau invoked the Emergencies Act (formerly known as the War Measures Act), for the first time since it became law in 1988. There were no reported acts of violence over three weeks despite hundreds of thousands of protestors in Otttawa.[38] Yet the Emergencies Act – only to be used to "preserve the sovereignty" of Canada or "acts of serious violence" – was invoked anyway.[39]

With the use of such powers, banks were mandated to freeze anyone suspected of being involved with the protestor's account. Digital technology made these bank freezes possible.

---

[35] J. R. Bruning, "A Revolution Under the Cloak of Normalcy", *Brownstone Institute*, 21 October 2022, <https://brownstone.org/articles/a-revolution-under-the-cloak-of-normalcy>.
[36] David G.W. Birch, "National Digital ID Is A Foundation For CBDC", *Forbes*, 26 April 2023, <https://www.forbes.com/sites/davidbirch/2023/04/26/national-digital-id-is-a-foundation-for-cbdc/?sh=74350e6b5a10>.
[37] WEF, "Future Focus 2025 Pathways for Progress from the Network of Global Future Councils 2020–2022", June 2022, <https://www3.weforum.org/docs/WEF_Future_Focus_2025.pdf>.
[38] Kurt Mahlburg, "Irony Abounds as Trudeau Declares War on Truckers", *Daily Declaration*, 17 February 2022, <https://dailydeclaration.org.au/2022/02/17/trudeau-declares-war-on-truckers/>.
[39] The Democracy Fund, "TDF releases legal brief for Canadian politicians on The Emergencies Act", 16 February 2022, "<https://www.thedemocracyfund.ca/the_emergencies_act_legal_guide>.

We include this example here for this reason: If a government can unlawfully use digital banking technology against its citizens without digital ID, what might be possible with it (and additional systems such as CBDC)?

4.4 Example of 'De-Banking' Nigel Farage

Nigel Farage, the former British politician made famous by his role in Brexit, was told by his private bank Coutts in June 2023 that his account was to be closed. *BBC News* ran the story that Farage was denied an account with Coutts due to falling "below the financial threshold" on 4 July.[40] Farage claimed that the account closure had to do with his political views, a claim that was vigorously denied. But the bank had lied.[41]

The *BBC N*ews piece was based on "a source familiar with Coutts", which turned out to be Coutts CEO Alison Rose. Amazingly, that same BBC article claimed that "Coutts said it did not comment on individuals' accounts" right after the author, Simon Jack, had met with Rose and discussed the financial reasons for closing Farage's account.[42] The BBC issued an apology on 21 July, stating that "considerations of his political views" were indeed among the reasons for the account termination.[43] CEO Alison Rose and the Coutts board mutually agreed her position was untenable, and she subsequently resigned.[44]

We include this example here for this reason. The idea that banks (or governments) would deny services to those deemed politically unworthy and enforce that digitally could be laughed out. But with Nigel Farage, that is exactly what happened. In the wrong hands, digital ID coupled with CBDC and even a social credit system will make these shameful scenarios far, far worse.

---

[40] Simon Jack & Daniel Thomas, "Nigel Farage bank account shut for falling below wealth limit, source tells BBC", *BBC News*, 20 July 2023, <https://www.bbc.com/news/business-66097039>.
[41] James Tapsfield, "Ministers back Farage after full Coutts dossier is revealed: Cancelling of ex-Ukip leader's account branded 'sinister' and a 'disgrace' after secret files show bank admitting he DID meet 'commercial criteria' but views were 'at odds' with 'inclusivity'", *Daily Mail*, 19 July 2023, <https://www.dailymail.co.uk/news/article-12314423/The-Coutts-Farage-dossier-bank-admitted-ex-Ukip-leader-DID-meet-commercial-criteria-used-tweet-Ricky-Gervais-trans-joke-Novak-Djokovic-ties-decide-odds-position-inclusive-organisation.html>.
[42] Anna Isaac and Kalyeena Makortoff, "NatWest boss Alison Rose resigns over Nigel Farage Coutts accounts row", *The Guardian*, 26 July 2023, <https://www.theguardian.com/business/2023/jul/26/natwest-boss-alison-rose-nigel-farage-account-coutts>.
[43] Jack & Thomas, "Nigel Farage bank account shut for falling below wealth limit, source tells BBC".
[44] Isaac and Makortoff, "NatWest boss Alison Rose resigns over Nigel Farage Coutts accounts row".

5.0 Conclusions and Recommendations

This submission has not made specific recommendations on how to improve the Digital ID Bill 2023, for the simple reason that we believe the project to be headed in the wrong direction. Therefore, we reject the Bill. We have raised the issue of the security of a centralised system, along with the increase of information and power such a system would bring. In addition, historical examples including the Aadhaar number in India were given to demonstrate how such systems can be misused and abused. The rights, dignity and privacy of the individual are preeminent, and any digital system must conform to these realities.

Instead, we recommend avoiding a centralised ID system and call for a thorough review into how best to protect the sensitive and private data of Australian citizens. We currently have various IDs (e.g. Medicare, driver's licence, tax file number, passports) that are all working well, with various security safeguards in place. A centralised system is not something Australian citizens asked for or was put on the table at the previous election.

A previous iteration of the digital ID bill was the Trusted Digital Identity Bill, which aimed to implement the Trusted Digital Identity Framework (TDIF), a centralised digital ID system for Australia. In December 2020 the Federal Government was informed via a consultation submission that the TDIF as designed had considerable security issues.[45] Instead of the TDIF, the authors (Ben Frengley and Vanessa Teague) recommended that the government pursue a public key infrastructure (PKI)-based system. They state:

> "A PKI-based system such as those used widely in the European Union is a promising alternative to the brokered model. PKI-based digital identity management is widespread and well understood, with published standards for international interoperability. It offers many of the security and privacy benefits that the TDIF aims to have, but with the added advantage that there is no entity who can meaningfully track user activity, as authentication occurs without the direct involvement of a central authority."[46]

[45] Rocco Loiacono and Phil Glover, "In digital ID we trust?", *Spectator Australia*, 28 October 2021, <https://www.spectator.com.au/2021/10/in-digital-id-we-trust/>.
[46] Ben Frengley and Vanessa Teague, "Submission to the Consultation on Digital ID", January 2023, <https://www.digitalidentity.gov.au/sites/default/files/2021-01/consultation01-vanessa-teague.pdf>: 2–3.

Their recommendation is as relevant as ever, and we commend their proposal seriously to the Committee. Unfortunately, it appears the previous government did not take such a promising course of action.

We repeat that while "protecting our digital identities is a welcome and well-overdue part of this proposed bill, getting it wrong could lead to harm at an even larger scale."[47] This is but one of the many reasons we reject this bill.

[47] Erica Mealy, "A national digital ID scheme is being proposed. An expert weighs the pros and (many more) cons", *The Conversation*, 26 September 2023, <https://theconversation.com/a-national-digital-id-scheme-is-being-proposed-an-expert-weighs-the-pros-and-many-more-cons-214144>.