

A national digital ID scheme is being proposed in Australia—an expert weighs the pros and (many more) cons

September 26 2023, by Erica Mealy



Credit: AI-generated image ([disclaimer](#))

In 2018-19, identity crime directly and indirectly cost Australia [an estimated](#) A\$3.1 billion.

To address such costs, the federal [government](#) is proposing a national

digital identity scheme that will let people [prove their identity](#) without having to share documents such as their passport, drivers license or Medicare card.

Finance Minister Katy Gallagher [opened consultations](#) for the [draft bill](#) last week, with plans to introduce the legislation to parliament by the end of the year.

Let's look at what it proposes, and what it could mean for you.

What would change?

The digital ID scheme would initially be regulated by the Australian Competition and Consumer Commission and the Australian Information Commissioner, with a view to eventually establish a new governing body.

The draft bill package includes strong updates to security requirements for how organizations store people's IDs, as well as the reporting of data breaches and suspected identity fraud.

In her [speech to](#) the Australian Information Industry Association, Gallagher outlined a four-phase rollout.

- Phase one: establishing the legislation and accreditation of private and public providers.
- Phase two: adding state- and territory-issued IDs to the scheme for use with federal government services.
- Phase three: bringing recognition of the digital ID into the [private sector](#). This would, for instance, allow you to use your digital ID to apply for a bank loan without having to provide your identity documents or copies.
- Phase four: allowing accredited private sector digital IDs to help verify you when accessing certain [government services](#).

How would it work?

For the [general public](#), the voluntary scheme would come in the form of a [smartphone app](#), requiring biometric information (such as a face print) to be unlocked.

To prove your identity to a participating organization, you would log into the organization's website and select [MyGovID](#) as your verification method.

You would then log into your MyGovID app and give consent for your identity to be verified with that organization. In this way, you could verify your identity to the organization without needing to share your drivers license, passport or similar.

Gone will be the days of 100 points of ID and copies of documents stored all over the internet.

The upside of the proposal

The [Medibank](#), [Optus](#) and [Latitude](#) data breaches of 2022–23 have demonstrated the lack of regulation and enforcement of identity protection legislation in Australia.

A welcome part of the draft bill is the increased power given to the Australian Information Commissioner, as well as restrictions on how organizations request, store and disclose people's [personal identifying information](#).

The bill also outlines minimum cybersecurity standards, and requires regular review of organizations dealing with identity data.

Unresolved MyGovID security flaws

In releasing the draft bill, the government has highlighted a voluntary national digital identity—the MyGovID—which is already [being used by](#) more than 6 million Australians and 1.3 million businesses.

MyGovID is a government-issued authenticator app which verifies your identity using one of three factors: something you know (such as a password), something you are (such as a biometric scan), or something you have (such as a verified phone number, where you can receive one-time codes). Adding additional factors makes verification more secure.

In 2020, security researchers warned the public [against using MyGovID](#) due to security flaws in its design. It's unclear if these have been addressed. The Australian Tax Office [declined to fix](#) the issue when raised.

Governments in Australia also have a [poor track record](#) of securing our information.

According to [Webber Insurance](#), 14 of the 44 recorded data breaches between January to June this year were reported by government authorities. These included the Department of Home Affairs, and the Northern Territory, Tasmania, ACT and NSW governments.

This is on top of [data breaches involving](#) the Australian Tax Office, National Disability Insurance Scheme and MyGov, as reported by the ABC last year.

More worryingly, the [privacy act](#) has a loophole which allows state and government authorities to remain exempt from compulsory data breach reporting. As such, we don't know just how many government data breaches have occurred.

The draft bill explicitly maintains these loopholes, [stating](#) entities are exempt from data reporting if "the entity is a department or authority of a State or Territory".

A honey trap for hackers

Even if the government carries out its end of the bargain securely, 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.

Also, streamlining distributed identification systems in this way will create an irresistible target for hackers. In cybersecurity this is called a [honeypot](#), or honey trap.

Just as honey is irresistible to bears, these data lures are irresistible to hackers. Failure to secure the data would make it a one-stop-shop for identity theft and extortion.

Perhaps most concerning is how closely the proposed scheme resembles government surveillance. By linking all our personal identification data across federal and state jurisdictions, as well as private entities, we would be giving the [federal government](#) complete oversight of our lives.

Small changes to the law, such as those [quietly made in](#) the Surveillance Legislation Amendment (Identify and Distrust) Act in 2021, could mean our locations could be tracked, and all our interactions with public and private organizations recorded.

What can you do?

It's clear the draft bill has a number of issues. That said, all hope is not

lost.

The government has committed to genuine consultation on its proposal. However, you don't have much time to [have your say](#): public submissions are being sought until October 10.

This extremely short consultation period doesn't provide much confidence a fit-for-purpose solution will be created.

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.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: A national digital ID scheme is being proposed in Australia—an expert weighs the pros and (many more) cons (2023, September 26) retrieved 11 May 2024 from <https://techxplore.com/news/2023-09-national-digital-id-scheme-australiaan.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--