



# Blind Citizens Australia

Ph 1800 033 660 | E [bca@bca.org.au](mailto:bca@bca.org.au) | W [bca.org.au](http://bca.org.au) | ABN 90 006 985 226

---

## Feedback on the Digital ID Bill 2023 and the Digital ID Rules 2024

Lodged via: <https://www.digitalidentity.gov.au/have-your-say/2023-digital-id-bill-and-rules-submissions>

Author: Dr Corey Crawford, National Policy Officer



10th October 2023

# Contents

---

Feedback on the Digital ID Bill 2023 and the Digital ID Rules 2024 .....	1
Contents.....	2
1. Introduction .....	2
1.1 About Blind Citizens Australia (BCA) .....	2
1.2 About people who are blind or vision impaired .....	3
2. Submission Context .....	3
3. Blind Citizens Australia's Submission .....	4
3.1 Lessons from the Director ID debacle.....	4
3.2 Ensuring biometric accessibility .....	6
3.3 Bolstering cybersecurity.....	7
4. Recommendations .....	9

## 1. Introduction

---

### 1.1 About Blind Citizens Australia (BCA)

Blind Citizens Australia (BCA) is the peak national representative organisation of and for the over 500,000 people in Australia who are blind or vision impaired. For nearly 50 years, BCA has built a strong reputation for empowering Australians who are blind or vision impaired to lead full and active lives and to make meaningful contributions to our communities. BCA provides peer support and individual advocacy to people who are blind or vision impaired across Australia.

Through our campaign work, we address systemic barriers by promoting the full and equal participation in society of people who are blind or vision impaired. Through our policy work, we provide advice to community and governments on issues of importance to people who are blind or vision impaired. As a disability-led organisation, our work is directly informed by lived experience. All directors are full members of BCA and the majority of our volunteers and staff are blind or vision

impaired. They are of diverse backgrounds and identities.

## 1.2 About people who are blind or vision impaired

There are currently more than 500,000 people who are blind or vision impaired in Australia with estimates that this will rise to 564,000 by 2030. According to Vision Initiative, around 80 per cent of vision loss in Australia is caused by conditions that become more common as people age.<sup>1</sup>

Australians who are blind or vision impaired can live rich and active lives and make meaningful contributions to their communities: working, volunteering, raising families and engaging in sports and other recreational activities. The extent to which people can actively and independently participate in community life does, however, rely on facilities, services and systems that are available to the public being designed in a way that makes them inclusive of the needs of all citizens – including those who are blind or vision impaired.

## 2. Submission Context

---

BCA welcomes the opportunity to provide feedback on the Commonwealth government's proposed legislation for an economy-wide digital identification (ID) system. The legislation consists of the Digital ID Bill 2023 and the Digital ID Rules 2024.

BCA's submission is based on the following legislative and policy frameworks, noting gaps in the fulfilment of requirements laid out in existing arrangements:

- Digital ID Bill 2023 (Cth).
- Digital ID Rules 2024 (Cth).
- Digital Economy Strategy 2030.
- Australia's Disability Strategy 2021–2031.
- United Nations Convention on the Rights of Persons with Disabilities (UNCRPD), particularly 'Article 9 – Accessibility.'

In recent years, governments across Australia have taken steps to improve the lives and experiences of people with disability. As a signatory to the UNCRPD,

governments in Australia have an obligation to protect and promote the human rights of people with disability.

The UNCRPD's 'Article 9 – Accessibility' requires State Parties to 'take appropriate measures to ensure to persons with disabilities access, on an equal basis with others, ... to information and communications, including information and communications technologies and systems.'<sup>2</sup>

According to the Commonwealth's Digital Economy Strategy 2030, Australia's economy could benefit from digitalisation by as much as \$315 billion over the next decade.<sup>3</sup>

Digitalisation can help people with disability to reach their employment potential. The World Economic Forum has identified educational technology, financial technology, social networking and remote working as important tools for levelling the playing field for people with disability in the workforce.<sup>4</sup>

Australia's Disability Strategy 2021–2031 lists Employment and Financial Security at the very top of seven Outcome Areas that need to be improved.<sup>5</sup> Inclusive digitalisation would benefit the economy at large and the 18 per cent of Australians (about 4.4 million people) who have some form of disability.<sup>6</sup>

Australia's digital transition has been hampered in recent years by major data breaches and increasingly sophisticated fraud technologies. These setbacks have highlighted the need for stronger digital ID verification.

## **3. Blind Citizens Australia's Submission**

---

### **3.1 Lessons from the Director ID debacle**

#### **General accessibility deficiencies**

In developing and rolling out the voluntary Australian Government Digital ID System, the Commonwealth cannot afford to repeat the many mistakes it made during the mandatory Director ID process in 2022.

A combination of technical bugs, difficulties accessing the myGov ID system, and overwhelmed customer service lines prevented some 700,000 company directors from signing up by the original 30th November deadline.<sup>7</sup>

Directors had to create a myGov ID before applying for a Director ID. Many applicants had their applications stalled by error codes and other problems with the myGov ID app. Accessing the myGov ID system was even more difficult for those without a smartphone.<sup>8</sup>

The Australian Taxation Office (ATO) and the Australian Business Registry Services (ABRS) made Director IDs mandatory for every person covered by the Corporations Act, encompassing many small businesses, charities and not-for-profit organisations. Unfortunately, the accessibility requirements of directors from organisations like BCA were not considered.

### Exclusion of people who are blind or vision impaired

The myGov ID registration process and the paper form alternative were both inaccessible for BCA's directors and chief executive officer, none of whom have a driver's licence and only a select few of whom have a passport.

The myGov ID system was exceedingly difficult to navigate for those BCA directors who have a small amount of functional sight and a passport. For those who do not have a passport or any functional sight, the process of applying for a 'Strong' myGov ID was simply impossible without sighted assistance.

Sally Karandrews, BCA's CEO, wrote to the ABRS about these accessibility barriers and followed up several times. The ABRS did not respond to Sally's queries. The Commonwealth must learn from these errors and ensure that the Australian Government Digital ID System is accessible for **all** Australians.

The application process must meet the accessibility and functionality standards set out in the current Web Content Accessibility Guidelines (WCAG 2.0), with a provision to improve accessibility and functionality standards when the new guidelines (WCAG 3.0) are released.

Any alternate application processes must also be accessible – i.e., not a paper-based form. The ongoing management of Digital IDs by Digital ID providers must meet these same standards for accessibility and functionality.

Whilst acknowledging that state- and territory-based proof of age cards will eventually be incorporated into the Australian Government Digital ID System, people who are blind or vision impaired typically do not have a driver's licence and often do

not have a passport. Until a provision is made to include proof of age cards, many people who are blind or vision impaired will not be able to obtain a Digital ID.

### **Recommendations:**

1. Ensure the application process for the Australian Government Digital ID System meets the accessibility and functionality standards outlined in the current Web Content Accessibility Guidelines (WCAG 2.0).
2. Include a provision to improve the system's accessibility and functionality standards when the new guidelines (WCAG 3.0) are released.
3. Ensure that the ongoing management of Digital IDs by Digital ID providers meet these same standards for accessibility and functionality.
4. Develop accessible alternate application processes for people who are blind or vision impaired.
5. Hasten the incorporation of proof of age cards into the Australian Government Digital ID System.

## **3.2 Ensuring biometric accessibility**

Biometrics allow people to be identified and authenticated through their unique biological characteristics. Creating a 'Standard' Digital ID with myGov ID does not require biometric authentication.

To bolster a myGov ID to 'Strong', the user must take a selfie of their face, which is then matched with the photograph on their passport. Once the person's identity is verified, the photograph is deleted.<sup>9</sup>

Taking a selfie is a simple task for some people, but a very challenging one for people who are blind or vision impaired. International biometric researchers have found that the selfies taken by people who are blind or vision impaired 'are often blurred, off centre, sometimes only partially visible, and occluded in some cases.'<sup>10</sup>

The requirement for a good quality facial image will exclude many people who are blind or vision impaired from being able to obtain a 'Strong' Digital ID. It is incumbent on the Commonwealth to make the selfie component of the Australian Government Digital ID System more accessible.

The international researchers found the photographic quality of selfies improved considerably when people who are blind or vision impaired were given explicit

instructions on how to place their device and then provided with audio feedback during the capture process. The audio prompts involved a beeping sound from a nearby computer that increased in frequency and volume as the subject moved their head into focus.

Audio feedback poses accessibility problems for people with deafblindness and for people who are Deaf or hard of hearing. To address this, researchers from Spanish biometrics company FacePhi have worked on facial recognition technology that uses vibration prompts to guide users to the centre of the screen when scanning their face.<sup>11</sup>

Both audio and vibration prompts should be incorporated into the selfie component of the Australian Government Digital ID System. This would allow all users to create a 'Strong' Digital ID and make Australia a global trendsetter in digital inclusion.

The Commonwealth could also explore other biometric options for crosschecking identity. For example, more than 7.1 million people already have their voiceprint verified by the ATO.<sup>12</sup> Incorporating secure voice authentication into the Australian Government Digital ID System could allow people who are blind or vision impaired to obtain a 'Strong' Digital ID without needing to take a selfie.

#### **Recommendations:**

6. Make the selfie component of the Australian Government Digital ID System more accessible by providing applicants with explicit instructions on how to place their device.
7. Provide applicants with audio and vibration prompts when taking their selfie.
8. Consider non-photographic biometric options for crosschecking identity, such as voice authentication.

### **3.3 Bolstering cybersecurity**

#### **Securing biometric data**

The Commonwealth has cited 'recent cyber events' as the catalyst for the proposed Digital ID legislation.<sup>13</sup> It is essential that the solution does not create even greater problems.

It is reassuring that the Australian Government Digital ID System is not built entirely upon biometric authentication. Temporary or permanent bodily changes may prevent a 100 per cent match for biometric indicators.<sup>14</sup>

This means that passwords and personal identification numbers (PINs) – which are either definitively correct or not – remain an essential part of digital security. Despite growing advances in technology, there also remains a role for human verification of digital information in order to ensure accuracy and prevent mistakes.

The Commonwealth insists that once the applicant's identify is verified, their photograph will be deleted from the Australian Government Digital ID System. To keep this promise, the Commonwealth must ensure its cybersecurity defences are as strong as possible.

Cybercriminals and adverse state actors are waiting to pounce on any mistakes made by Australian officials. As cybersecurity expert Adrianus Warmenhoven warns, 'all recorded data is hackable.' This includes biometric information, which is a 'valuable target for cybercriminals.'<sup>15</sup>

Inadequate cyber protections can expose millions of unsuspecting people. In 2019, two cybersecurity researchers gained access to 27.8 million records and 23 gigabytes-worth of data – including fingerprint data and facial recognition data – from Biostar 2's poorly defended database.<sup>16</sup> Biostar 2's services are used by the United Kingdom's banks, defence contractors and Metropolitan Police Service.

Government databases can also be directly breached, as was the case during the 2015 hack of the United States Office of Personnel Management by an adverse state actor. The fingerprints of 5.6 million American federal government employees were stolen during that data breach, seriously endangering the national security of the United States.<sup>17</sup>

### Addressing outstanding problems

Some of the dangers of lax cybersecurity have already been exposed in Australia. In 2020, two cybersecurity researchers informed the Australian Signals Directorate of a crucial design flaw in the myGov ID app.<sup>18</sup> The ATO declined to fix the problem when informed.<sup>19</sup>



It remains unclear if the design flaw has been rectified. For myGov ID users to have confidence in the platform, any outstanding cybersecurity flaws must be fixed immediately.

The credibility of the ATO has again come into question regarding its voice authentication system, which it describes as 'both a reliable and secure way of confirming your identity.'<sup>20</sup> As noted in section 3.2, voice authentication could provide an alternative to taking selfies for people who are blind or vision impaired.

It is unfortunate, then, that a journalist was recently able to use an artificial intelligence-generated clone of their voice to gain access to their own Centrelink self-service account.<sup>21</sup>

Continuing the poor track record of governmental cybersecurity, the Australian Defence Force, the Department of Home Affairs, and various state and territory authorities have featured in data breaches and cyberattacks this year.<sup>22</sup>

For people to feel confident enough to provide biometric information for authentication purposes, Commonwealth, state and territory authorities must improve their cybersecurity defences.

#### **Recommendations:**

9. Ensure that the Australian Government Digital ID System does not become entirely dependent upon biometric authentication.
10. Guarantee that biometric information is actually deleted at the designated time.
11. Maintain strong cybersecurity defences to protect the Australian Government Digital ID System.
12. Immediately fix any outstanding cybersecurity flaws in the myGov ID system.
13. Work with state and territory authorities to improve governmental cybersecurity defences.

## **4. Recommendations**

---

To create an Australian Government Digital ID System that is trustworthy and inclusive of all Australians, the Commonwealth must:

1. Ensure the application process for the Australian Government Digital ID System meets the accessibility and functionality standards outlined in the current Web Content Accessibility Guidelines (WCAG 2.0).
2. Include a provision to improve the system's accessibility and functionality standards when the new guidelines (WCAG 3.0) are released.
3. Ensure that the ongoing management of Digital IDs by Digital ID providers meet these same standards for accessibility and functionality.
4. Develop accessible alternate application processes for people who are blind or vision impaired.
5. Hasten the incorporation of proof of age cards into the Australian Government Digital ID System.
6. Make the selfie component of the Australian Government Digital ID System more accessible by providing applicants with explicit instructions on how to place their device.
7. Provide applicants with audio and vibration prompts when taking their selfie.
8. Consider non-photographic biometric options for crosschecking identity, such as voice authentication.
9. Ensure that the Australian Government Digital ID System does not become entirely dependent upon biometric authentication.
10. Guarantee that biometric information is actually deleted at the designated time.
11. Maintain strong cybersecurity defences to protect the Australian Government Digital ID System.
12. Immediately fix any outstanding cybersecurity flaws in the myGov ID system.
13. Work with state and territory authorities to improve governmental cybersecurity defences.

---

<sup>1</sup> Vision 2020 Australia, "Eye Health in Australia," accessed 31 January 2023, <http://www.visioninitiative.org.au/common-eye-conditions/eye-health-in-australia>

<sup>2</sup> United Nations, "Conventions on the Rights of Persons with Disabilities (UNCRPD) – Article 9," 13 December 2006, <https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities/article-9-accessibility.html>

<sup>3</sup> Australian Government, "Digital Economy Strategy: A Leading Digital Economy and Society by 2030," May 2021, <https://apo.org.au/sites/default/files/resource-files/2021-05/apo->

---

[nid312247.pdf](#)

<sup>4</sup> World Economic Forum, “Technology Can Level the Playing Field for People with Disabilities in the Workforce,” 5 July 2021, <https://www.weforum.org/agenda/2021/07/digital-technology-workforce-disabled-people/>

<sup>5</sup> Disability Gateway, “Australia’s Disability Strategy 2021–2031,” December 2021, <https://www.disabilitygateway.gov.au/sites/default/files/documents/2021-11/1781-australias-disability.docx>

<sup>6</sup> Australian Institute of Health and Welfare, “Prevalence of Disability,” 5 July 2022, <https://www.aihw.gov.au/reports/disability/people-with-disability-in-australia/contents/people-with-disability/prevalence-of-disability>

<sup>7</sup> SmartCompany, “‘Bring on the Fine’: Business Leaders See Red Over Director ID Application Bugs,” SmartCompany, 2 December 2022, <https://www.smartcompany.com.au/business-advice/director-id-application-bugs-mygovid-ato/>

<sup>8</sup> Ibid.

<sup>9</sup> Australian Government, “How Digital ID Works,” accessed 28 September 2023, <https://www.digitalidentity.gov.au/how-digital-id-works>

<sup>10</sup> Norman Poe et al., “Blind Subjects Faces Database,” IET Biometrics, March 2016, <https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-bmt.2015.0016>

<sup>11</sup> Vice, “Facial Recognition Apps Are Leaving Blind People Behind,” 16 March 2016, <https://www.vice.com/en/article/ezpzzp/facial-recognition-apps-are-leaving-blind-people-behind>

<sup>12</sup> The Guardian, “AI Can Fool Voice Recognition Used to Verify Identity by Centrelink and Australian Tax Office,” 17 March 2023, <https://www.theguardian.com/technology/2023/mar/16/voice-system-used-to-verify-identity-by-centrelink-can-be-fooled-by-ai>

<sup>13</sup> Australian Government, “Digital ID Bill – What Is It?” September 2023, [https://www.digitalidentity.gov.au/sites/default/files/2023-09/australias\\_digital\\_id\\_system\\_legislation\\_factsheet.pdf](https://www.digitalidentity.gov.au/sites/default/files/2023-09/australias_digital_id_system_legislation_factsheet.pdf)

<sup>14</sup> Forbes, “Hacking Our Identity: The Emerging Threats from Biometric Technology,” 9 March 2019, <https://www.forbes.com/sites/cognitiveworld/2019/03/09/hacking-our-identity-the-emerging-threats-from-biometric-technology/?sh=126fb12b5682>

<sup>15</sup> Quoted in TechRadar, “Your Biometrics May Not Be As Safe As You Think,” 22 August 2023, <https://www.techradar.com/pro/security/your-biometrics-may-not-be-as-safe-as-you-think>

<sup>16</sup> The Guardian, “Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms,” 14 August 2019, <https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms>

<sup>17</sup> The Guardian, “US Government Hack Stole Fingerprints of 5.6 Million Federal Employees,” 24 September 2015, <https://www.theguardian.com/technology/2015/>

---

[sep/23/us-government-hack-stole-fingerprints](#)

<sup>18</sup> iTnews, “Researchers Say Not to Use myGov ID Until Login Flaw is Fixed,” 21 September 2020, <https://www.itnews.com.au/news/researchers-say-not-to-use-mygovid-until-login-flaw-is-fixed-553601>

<sup>19</sup> Erica Mealy, “A National 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>

<sup>20</sup> Australian Taxation Office, “Voice Authentication,” 29 June 2021, <https://www.ato.gov.au/General/Online-services/Voice-authentication/>

<sup>21</sup> The Guardian, “AI Can Fool Voice Recognition Used to Verify Identity by Centrelink and Australian Tax Office.”

<sup>22</sup> Webber Insurance Services, “The 2023 Data Breach Notifications in Australia,” accessed 4 October 2023, <https://www.webberinsurance.com.au/data-breaches-list#twentythree>