Blind Citizens Australia

Ph 1800 033 660 | E bca@bca.org.au | W bca.org.au | ABN 90 006 985 226

Submission to the Senate Economics Legislation Committee's Inquiry into Digital ID Bill 2023

Lodged via: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/DigitalIDBills2023

Author: Dr Corey Crawford, National Policy Officer

[redacted]

18th January 2024

Contents

Blind Citizens Australia

1. Introduction

1.1 About Blind Citizens Australia

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.[1]

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 – including those who are blind or vision impaired.

2. Submission Context

BCA welcomes the opportunity to make a submission to the Senate Economics Legislation Committee's Inquiry into the Digital ID Bill 2023. This submission builds on BCA's earlier feedback on the Commonwealth government's proposed legislation for an economy-wide digital identification (ID) system.[2]

BCA's submission is based on the following legislative and policy frameworks:

- Digital ID Bill 2023 (Cth).
- Digital ID (Transitional and Consequential Provisions) 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.'[3]

According to the Commonwealth government's Digital Economy Strategy 2030, Australia's economy could benefit from digitalisation by as much as $315 billion over the next decade.[4]

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.[5]

Australia's Disability Strategy 2021–2031 lists Employment and Financial Security at the very top of seven Outcome Areas that need to be improved.[6]

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.[7]

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 Director ID

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.[8]

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.[9]

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. Regrettably, 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 then-Chief Executive Officer, 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 2.1), 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 may 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 2.1).
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 for all Australians

Facial recognition's risk of discrimination

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.[10]

Researchers from the Human Technology Institute at the University of Technology Sydney have warned that facial recognition technologies are 'imperfect,' carry 'significant risk' and 'unavoidably [restrict] the right to privacy.'[11]

The risk includes 'algorithmic bias and errors, including demographic variations in error rates, which can lead to discrimination, misidentification or failure to identify an individual' and the subsequent 'denial of access to basic services and entitlements.'[12]

The Commonwealth government has appointed the Australian Competition and Consumer Commission (ACCC) as the initial Digital ID Regulator, to be replaced by a digital-specific regulator as the Digital ID System expands over time.[13]

The Commonwealth should establish a streamlined pathway that allows people to complain directly to the ACCC/digital-specific regulator when they believe they have experienced discrimination or misidentification at the hands of the Digital ID System.

In previous submissions, BCA has noted the many barriers faced by complainants when reporting discrimination by state- and territory-based transport operators and providers.[14]

Given the government's stated intention for the Digital ID System to be used for Commonwealth, state, territory and private sector services, complainants must be

given the ability to complain directly to the ACCC/digital-specific regulator, and for cases to be investigated and resolved speedily.

Without a streamlined complaints pathway, complainants would instead have to pursue recourse through the Australian Human Rights Commission (AHRC). The complainant could be denied access to vital government and private sector services in the months or years it took for the AHRC to adjudicate.

Recommendation:

6. Establish a streamlined complaints pathway that allows the Australian Competition and Consumer Commission (ACCC)/digital-specific regulator to speedily investigate complaints of Digital ID-related discrimination or misidentification.

Make selfies more accessible

Taking a selfie is a simple task for some people, but a particularly 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.'[15]

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.[16]

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.[17] 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:

7. 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.
8. Provide applicants with audio and vibration prompts when taking their selfie.
9. Consider non-photographic biometric options for crosschecking identity, such as voice authentication.

3.3 Bolstering cybersecurity protections

Securing users' biometric data

In November 2023, it was reported that nearly half of all Australian adults had been affected by a data breach in the previous 12 months.[18] The Commonwealth has cited 'recent cyber events' as the catalyst for the proposed Digital ID legislation.[19] 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.[20]

This means that passwords and personal identification numbers (PINs) – which are either definitively correct or not – must remain an essential part of digital security.[21] 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 particularly 'valuable target for cybercriminals.'[22]

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 and facial recognition data – from Biostar 2's poorly defended database.[23] 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.[24]

Recommendation:

10. Ensure that biometric information is actually deleted at the designated time.

Addressing Australia's major cybersecurity flaws

In 2013, it was revealed that an adverse state actor had stolen the blueprints for the new headquarters of the Australian Security Intelligence Organisation.[25] The inability to protect even the nation's largest and most powerful intelligence agency raises questions about the Commonwealth's capacity to defend a centralised ID database, which will doubtless be a highly attractive target for hackers.

Numerous reports by auditors-general at both Commonwealth and state level have highlighted the problems Australian governments have with data security.[26] Governments have demonstrated an unwillingness or inability to address these issues, allowing high-profile hacks and data breaches to occur with alarming regularity.

In 2020, for example, two cybersecurity researchers informed the Australian Signals Directorate of a crucial design flaw in the myGov ID app.[27] The ATO declined to fix the problem when informed.[28]

It remains unclear if the design flaw has been rectified. For myGov ID users to have confidence in the platform, it is imperative that any outstanding cybersecurity flaws are rectified 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.'[29] As noted in section 3.2 of this submission, 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.[30]

Continuing the poor track record of governmental cybersecurity, the Australian Defence Force, the Department of Home Affairs, the National Disability Insurance Agency, and various state and territory authorities experienced significant data breaches and/or cyberattacks in 2023.[31]

For people to feel confident enough to provide biometric and other deeply personal information for authentication purposes, Commonwealth, state and territory authorities must greatly strengthen their cybersecurity defences.

Recommendations:

11. Immediately fix any outstanding cybersecurity flaws in the myGov ID system.
12. Develop stronger cybersecurity defences to protect the Australian Government Digital ID System specifically.
13. Work with state and territory authorities to improve governmental cybersecurity defences more generally.

3.4 Building and maintaining the public's confidence

Promoting the new Digital ID System

Canstar research recently commissioned by the Commonwealth government found that Australians want to protect their personal data, but that they still lack an understanding of the concept behind the Australian Government Digital ID System. In order for the new system to be successful, the Commonwealth must do a better job of explaining and promoting its benefits.[32]

Recommendation:

14. Increase public promotion of the Australian Government Digital ID System.

Learning from COVID-era mistakes

Having built the public's understanding and confidence in the Australian Government Digital ID System, the Commonwealth must then ensure the system is used 'for the advertised purpose, and nothing else.'[33] The Commonwealth cannot afford to repeat the mistakes made at the state level during the COVID-19 pandemic, which undermined the public's confidence in contact tracing systems.

In November 2020, the then-Premier Mark McGowan promised that the SafeWA contact tracing smartphone app would 'be encrypted at the point of capture, stored securely and only be accessible by authorised Department of Health contact tracing personnel, should COVID-19 contact tracing be necessary.'[34]

By June 2021, however, WA Health had received six orders from the Western Australia Police Force to produce SafeWA information for policing purposes, and an additional request which did not result in a formal order.[35]

WA Health granted access in response to three of those orders before the Western Australian government passed urgent legislation to prevent this from occurring.[36] The legislation was required after the Western Australian Police Commissioner ignored the Premier's personal request that police stop seeking access to SafeWA information.[37]

Despite the government's assurances to the public, the Commissioner said that police officers would continue the practice until it was made expressly unlawful. The

Premier put the legislative loophole down to the app being 'created very, very quickly' during the pandemic.[38]

Victoria Police similarly sought access to QR code check-in data three times in December 2020 as part of criminal investigations. However, these requests were rebuffed by the Department of Health and Service Victoria.[39]

Privacy and civil liberties advocates are concerned that the Commonwealth may be repeating the Western Australian mistake.[40] In a background briefing on 30th November 2023, Commonwealth officials confirmed that Australia's intelligence agencies would not need a warrant to access data linked to the Australian Government Digital ID System.[41]

Recommendation:

15. Stipulate in the legislation that the Australian Government Digital ID System can be used only for its advertised purpose, and nothing else.

Ensuring viable platforms for non-Digital ID users

In her second reading speech, Finance Minister Katy Gallagher made the following statement:

> An essential safeguard in the Bill is that Digital ID will continue to be voluntary for individuals accessing government services through the Australian Government Digital ID System. The Bill will require Australian Government agencies to continue to provide alternate channels for people to access services.[42]

As previously noted, the myGov ID platform is currently not accessible for many people who are blind or vision impaired. Though BCA is hopeful the Digital ID System will be fully accessible for all Australians who want to participate, there must be viable alternate platforms for people to access government services when they are unable or unwilling to sign up for a Digital ID.

Providing people with a genuine choice of platforms, whilst informing them of the benefits of Digital ID, would allow people to feel that the new system is not being foisted on them. This could help arrest the recent slump in Australians' trust in government.[43]

Recommendation:

16. Provide people unable or unwilling to sign up for a Digital ID with a genuine choice of platforms to access government services.

4. Summary of Recommendations

In reviewing the Digital ID Bill 2023, the Senate Economics Legislation Committee should consider BCA's following recommendations to the Commonwealth government:

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 2.1).
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. Establish a streamlined complaints pathway that allows the Australian Competition and Consumer Commission (ACCC)/digital-specific regulator to speedily investigate complaints of Digital ID-related discrimination or misidentification.
7. 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.
8. Provide applicants with audio and vibration prompts when taking their selfie.
9. Consider non-photographic biometric options for crosschecking identity, such as voice authentication.
10. Ensure that biometric information is actually deleted at the designated time.
11. Immediately fix any outstanding cybersecurity flaws in the myGov ID system.

12. Develop stronger cybersecurity defences to protect the Australian Government Digital ID System specifically.
13. Work with state and territory authorities to improve governmental cybersecurity defences more generally.
14. Increase public promotion of the Australian Government Digital ID System.
15. Stipulate in the legislation that the Australian Government Digital ID System can be used only for its advertised purpose, and nothing else.
16. Provide people unable or unwilling to sign up for a Digital ID with a genuine choice of platforms to access government services.

---

[1] Vision 2020 Australia, "Eye Health in Australia," accessed 23 November 2023, http://www.visioninitiative.org.au/common-eye-conditions/eye-health-in-australia

[2] Blind Citizens Australia, "Feedback on the Digital ID Bill 2023 and the Digital ID Rules 2024," 10 October 2023, https://www.bca.org.au/wp-content/uploads/2023/10/BCA-Feedback-on-Digital-ID-Bill-2023-and-Digital-ID-Rules-2024-v1.0.docx

[3] 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

[4] 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

[5] 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/

[6] 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

[7] 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

[8] 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/

[9] Ibid.

[10] Australian Government, "How Digital ID Works," accessed 28 September 2023, https://www.digitalidentity.gov.au/how-digital-id-works

[11] Edward Santow et al., "Improving Governance and Training for the Use of Facial Verification Technology in NSW Digital ID," James Martin Institute for Public Policy,

November 2023, https://jmi.org.au/wp-content/uploads/2023/12/JMI-PIP-Improving-governance-and-training-for-the-use-of-facial-verification-technology-in-NSW-Digital-ID.pdf

[12] Ibid.

[13] Herbert Smith Freehills, "The Australian Government Releases Exposure Draft of the Digital ID Bill," 11 October 2023, https://www.herbertsmithfreehills.com/insights/2023-10/the-australian-government-releases-exposure-draft-of-the-digital-id-bill

[14] Blind Citizens Australia, "Response to the 2022 Review of the Disability Standards for Accessible Public Transport 2002," 30 June 2023, https://www.bca.org.au/wp-content/uploads/2023/07/BCA-Response-to-the-Review-of-the-Disability-Transport-Standards-v1.0.docx

[15] Norman Poe et al., "Blind Subjects Faces Database," IET Biometrics, March 2016, https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-bmt.2015.0016

[16] 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

[17] 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

[18] Technology Decisions, "Half of Australians Hit By Data Breach in Past 12 Months," 30 November 2023, https://www.technologydecisions.com.au/content/security/news/half-of-australians-hit-by-data-breach-in-past-12-months-78648980

[19] 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

[20] 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

[21] Santow et al., "Improving Governance and Training for the Use of Facial Verification Technology in NSW Digital ID."

[22] 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

[23] 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

[24] 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

[25] The Sydney Morning Herald, "Blueprints for New ASIO Headquarters 'Stolen,'" 27 May 2013, https://www.smh.com.au/technology/blueprints-for-new-asio-headquarters-stolen-20130527-2n7kz.html

[26] The Mandarin, "Audits Reveal Weaknesses in Government Data Security," 11 November 2022, https://www.themandarin.com.au/205341-audits-reveal-weaknesses-government-data-security/

[27] 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

[28] 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

[29] Australian Taxation Office, "Voice Authentication," 29 June 2021, https://www.ato.gov.au/General/Online-services/Voice-authentication/

[30] The Guardian, "AI Can Fool Voice Recognition Used to Verify Identity by Centrelink and Australian Tax Office."

[31] Webber Insurance Services, "The 2023 Data Breach Notifications in Australia," accessed 20 December 2023, https://www.webberinsurance.com.au/data-breaches-list#twentythree

[32] BiometricUpdate.com, "Australians Do Not Understand Incoming Digital ID System," 17 November 2023, https://www.biometricupdate.com/202311/australians-do-not-understand-incoming-digital-id-system

[33] Tama Leaver, "Police Debacle Leaves McGowan Government Battling to Rebuild Public Trust in the SafeWA App," The Conversation, 16 June 2021, https://theconversation.com/police-debacle-leaves-the-mcgowan-government-battling-to-rebuild-public-trust-in-the-safewa-app-162850

[34] Mark McGowan, "Facebook Page," 26 November 2020, https://www.facebook.com/MarkMcGowanMP/posts/4969401309744370?ref=embed_post

[35] Western Australian Auditor General's Report, "SafeWA – Application Audit," 2 August 2021, https://audit.wa.gov.au/wp-content/uploads/2021/07/Report_2__SafeWA-Application-Audit.pdf

[36] Ibid.

[37] iTnews, "WA Police Refused Request to Stop Accessing Covid Check-In App Data," 16 June 2021, https://www.itnews.com.au/news/wa-police-refused-request-to-stop-accessing-covid-check-in-app-data-566033

[38] Quoted in ibid.

[39] The Age, "Police Sought Access to QR Check-In Data Intended for Contact Tracing," 21 June 2021, https://www.theage.com.au/politics/victoria/police-sought-access-to-qr-check-in-

data-intended-for-contact-tracing-20210621-p582x4.html

[40] Mobile ID World, "Australian Government Moves to Expand Scope of Digital ID," 1 December 2023, https://mobileidworld.com/australian-government-moves-to-expand-scope-of-digital-id/

[41] The Mandarin, "Digital Identity Costs Hit $782 Million as New Laws Introduced," 1 December 2023, https://www.themandarin.com.au/235775-digital-identity-costs-hit-782-million-as-new-laws-introduced/

[42] Katy Gallagher, "Senate Hansard: Digital ID Bill 2023, Digital ID (Transitional and Consequential Provisions) Bill 2023 Second Reading," 30 November 2023, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansards%2F27149%2F0098%22

[43] ABC News, "Trust Slumps in Government and Media as Division Rules, Edelman Survey Shows," 8 February 2023, https://www.abc.net.au/news/2023-02-08/trust-slump-as-division-rules/101939406