Submission to the Digital Transformation Agency

responding to the

Digital Identity Exposure Draft

27 October 2021

DIGITAL RIGHTS WATCH

Overview

We welcome the opportunity to submit comments to The Digital Transformation Agency (DTA) on the Digital Identity Exposure Draft.[1]

Over the past few months, we have been actively watching the development of the long-overdue Australian Privacy Act update. While the Privacy Act wouldn't necessarily reshape government use of digital identity, it would certainly impact the privacy practices and use of personal data by businesses and private institutions. We would encourage the DTA to consider waiting for the Privacy Act update and shaping the Digital Identity framework in line with what Australians expect of their privacy in the digital era; and not to defer this responsibility to the two year review of the Digital Identity framework.

Digital transformation is rapidly happening all around the globe and as governments rush to adopt digital identity programs and cards, increasing case studies show us the harm that an over-broad system without adequate safeguards can cause to human rights. It is because of this over-adoption trend that last year Digital Rights Watch joined dozens of civil society groups and hundreds of subject matter experts in calling on governments to reconsider the rampant adoption of digital identity systems under the banner of #WhyID.[2]

- UN Inquiry Into the Right to Privacy in a Digital Age https://digitalrightswatch.org.au/2018/04/10/submission-to-un-inquiry-into-the-right-to-privacy-in-a-digital-age/
- UN Human Rights Council Australia Universal Periodic Review https://digitalrightswatch.org.au/2020/08/28/access-now-and-digital-rights-watch-joint-submission-to-the-un-human-rights-council/
- WhyID open letter to governments considering digital identity solutions https://www.accessnow.org/whyid/

Digital Rights Watch

Digital Rights Watch is a charity organisation founded in 2016 whose mission is to ensure that people in Australia are equipped, empowered and enabled to uphold their digital rights. We stand for Privacy, Democracy, Fairness & Freedom in a digital age. We believe that digital rights are human rights which see their expression online.

We educate, campaign, and advocate for a digital environment where individuals have the power to maintain their human rights.[3]

---

[1] The exposure draft is available on the digital identity website: https://www.digitalidentity.gov.au/sites/default/files/2021-09/Trusted%20Digital%20Identity%20Bill%202021%20exposure%20draft.pdf

[2] Full text of the letter is available: https://www.accessnow.org/whyid/

[3] Learn more about our work on our website: https://digitalrightswatch.org.au/

General comments

There is a generalised assumption that certain kinds of digital identity programmes empower users, but there are many cases of harmful digital identity programmes around the world. In a 2019 report to the UN General Assembly, the Special Rapporteur on extreme poverty and human rights, Philip Alston, raised concerns about the emergence of the “digital welfare state”. He said that too often behind digital identity programs is the desire to slash welfare spending, set up intrusive government surveillance systems, and generate profits for private corporations who are tasked with building and maintaining the infrastructure.[4]

In his report, Rapporteur Alston specifically made the case that governments justified the introduction of expensive and complex biometric digital identity card systems on the grounds that they would improve welfare services and reduce fraud. "The process is commonly referred to as 'digital transformation' by governments and the tech consultancies that advise them, but this somewhat neutral term should not be permitted to conceal the revolutionary, politically-driven, character of many such innovations." His analysis of several case studies from around the globe lead him to conclude that these systems are used to automate, predict, identify, surveil, detect, target and punish, rather than offer the social security and protection they promise.

In spite of these risks, digital identity programmes continue to be pushed as a part of the development agenda at the international level by the World Bank. Australia actually plays a key partnership role in that space, and continues to promote initiatives like ID4D as part of its international development agenda.[5]

The ID4D initiative itself identifies several key risks in creating a good ID system, where it pinpoints not only several universal risks, but also key challenges to “low- and middle-income countries” several of which are worryingly applicable in the Australian context.[6] One of the factors in that category is **limited and poor connectivity** which continues to disproportionately impact certain communities in Australia (some of that is an overlap of connectivity and affordability). Another factor is **poor trust in government services**, which is an increasingly significant problem for all Australian digital projects, as evidenced by the opt-out rate of the My Health Record scheme.[7] The third-biggest factor in that category for Australia is **insufficient cybersecurity capacity**.

---

[4] The full statement and link to the report can be found on the OHCHR website (October 2019) https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25156

[5] “To accelerate the Initiative’s work at global, regional and country levels, the ID4D Multi-Donor Trust Fund (MDTF) was established with catalytic contributions from the Bill & Melinda Gates Foundation followed by the UK Government, the French Government, the Australian Government and the Omidyar Network.” https://id4d.worldbank.org/who-is-involved

[6] Creating a good ID system presents risks and challenges, ID4D, https://id4d.worldbank.org/guide/creating-good-id-system-presents-risks-and-challenges-there-are-common-success-factors

[7] More than 25 million people have opted out of my health record, Guardian (February 2019) https://www.theguardian.com/australia-news/2019/feb/20/more-than-25-million-people-have-opted-out-of-my-health-record

Existing Australian identity and trust challenges

The existing Australian digital identity infrastructure has been fraught with criticism and problems, most of which remain unaddressed. In all discussions about Australian digital identification, the Australia Card experience looms large, and newer iterations like Digital ID and GovPass have been designed deliberately to avoid the same pitfalls. To compound the issue of a lack of trust, existing initiatives have been plagued by vulnerabilities. Just last year Professor Vanessa Teague and Ben Frengley disclosed a weakness in its myGovID system to the Australian Taxation Office (ATO).[8] They found that myGovID is subject to an easily implemented code-proxying attack, which allows a malicious website to proxy a person's myGovID login and re-use their authentication to log into the victim's account on any website of their choice.

The Office of the Australian Information Commission (OAIC)'s polling gives a strong indication that Australians are sceptical to uptake government digital initiatives.[9] In the most recent (2020) Community Attitudes to Privacy survey, the biggest privacy risks identified by Australians were identity theft and fraud (76%), data security and breaches (61%), and digital services, including social media sites (58%). The survey also showed that since 2007, there has been a general downward trend in trust in personal information handling, including in companies in general (down by 13%) and in Federal Government departments (down 14%). This downward trend in trust towards the Federal Government is reflected in reality from the aforementioned opt-out of My Health Record to the sluggish uptake of the federal government's COVIDSafe app.[10]

The potential benefits of a robust and secure identity system are real. But at the end of the day, we need our government to put our rights ahead of the private sector, and ensure that people are not forced to trade their rights for convenience as part of a digitisation initiative.

Recommendations

- **Prioritise an update to the Privacy Act and the precedent it may set for privacy.** Given the topical overlap and potential for new privacy reforms to fundamentally change the way data protection and privacy is viewed in Australian legislation, it should remain a priority to anticipate an updated *Privacy Act* before proceeding with any other fundamental changes to the way that personal data of Australians is treated.

---

[8] ATO declines to fix code flaw within myGovID, ZDNet (Sept 2020)
https://www.zdnet.com/article/ato-declines-to-fix-code-replay-flaw-within-mygovid/

[9] Australian community attitudes to privacy, OAIC (2020)
https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/

[10] Privacy concerns and digital government: exploring citizen willingness to adopt the COVIDSafe app (May 2021)
https://www.tandfonline.com/doi/abs/10.1080/0960085X.2021.1920857?journalCode=tjis20

- **Introduce robust data protection and handling rules for accredited entities**. The exposure draft does not outline any expectations around how accredited entities shall treat the information they receive under the scheme. There should be a concrete requirement on not sharing the data with third parties (and data brokers), and not aggregating it or merging it with other datasets (we acknowledge the intent to limit speculative profiling, but that remains only a small part of the risks to individual's data).
- **The Oversight Authority (OA) should be split into two offices**. As drafted, the OA oversees the functionality and utility of the scheme, rather than oversight in the meaning of accountability and integrity. In order to ensure oversight to the functionality of the scheme, a single office must not be performing both functions.
- **Prohibit use of digital identity data for enforcement purposes.** In spite of overwhelming feedback from the public consultations on the digital identity framework to prohibit access to enforcement agencies, there is a large carveout in Section 81 of the exposure draft to give law enforcement access to data when there is "reasonable suspicion." **There should be no such access, under any circumstances.**
- **Do not integrate biometric data into the TDIF** in order to minimise risks to the individual and reduce the cybersecurity threat to the infrastructure.
- **Ensure that the digital identity framework remains truly voluntary.** Individuals should have a choice to opt into the scheme whether they are interacting with government services or private entities. All accredited private participants must accommodate alternative ways to interact with individuals who do not wish to use the scheme.
- **Maintain analogue pathways for individuals to interact with, and use, services**. There are many valid reasons due to which individuals may be unable to interact with the digital identity framework. Connectivity and network affordability may be one, digital literacy another. No services should be denied to them because of that.
- **Ensure that there are easy ways to alter consent, and delete or alter data.** Consent can be a complex issue, especially when individuals have no ability to choose between services or meaningfully opt out. The digital identity framework must allow for consent to be withdrawn (data to be deleted on the TDIF or accredited partner side), and simple pathways to delete or alter data if the individual wishes to do so.

Contact

Lucie Krahulcova | Executive Director | Digital Rights Watch | lucie@digitalrightswatch.org.au