Submission to the Digital ID Taskforce

regarding the

Digital ID Bill 2023 exposure draft

11 October 2023

DIGITAL RIGHTS WATCH

Who we are

Digital Rights Watch is a charity organisation founded in 2016 to promote and defend human rights as realised in the digital age. We stand for privacy, democracy, fairness and freedom. Digital Rights Watch educates, campaigns and advocates for a digital environment in which rights are respected, and connection and creativity can flourish. More information about our work is available on our website: www.digitalrightswatch.org.au

Acknowledgement of Country

Digital Rights Watch acknowledges the Traditional Owners of Country throughout Australia and their continuing connection to land and community. We acknowledge the Aboriginal and Torres Strait Islander peoples as the true custodians of this land that was never ceded and pay our respects to their cultures, and to elders past and present.

Contact

Samantha Floreani | Program Lead | [redacted]

General remarks

Digital Rights Watch welcomes the opportunity to provide comments to the Digital ID Taskforce regarding the exposure draft of the *Digital ID Bill 2023* and its corresponding draft Digital ID Rules 2024.

Over the years, Digital Rights Watch has actively participated in Australia's digital identity space. For example, we have participated in several roundtables with the Digital Transformation Agency and provided submissions throughout the development of the Trusted Digital Identity Framework, including:

- Submission to the Digital Transformation Agency in response to the Digital Identity Legislation Position Paper, July 2021
- Submission to the Digital Transformation Agency in response to the Digital Identity Exposure Draft, October 2021

In the past, we have also supported international human rights and civil society organisations campaigning for human rights, autonomy, dignity and agency of people in digital identification systems, such as the #WhyID campaign.

Over the years, we have remained critical of rapid digital transformation programs, including the rollout of digital identity systems, without due regard to the protection of human rights. Across the globe, there are increasing case studies that show the harm that overly-broad systems without adequate safeguards can produce. Perhaps the most prominent example is the Aadhaar system in India, which is linked to social services and was designed to improve accessibility to certain services. However the system has been subject to court cases and scrutiny, and was found to create discrimination and surveillance of marginalised groups, and had severe security vulnerabilities which led to data being extracted and exploited.[1]

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.[2]

It is with this context in mind that Digital Rights Watch has been, and to date remains, critical of digital identity programs and their potential to undermine human rights, enable surveillance, create dangerous digital security

[1] Supreme Court of India rules to restrict the world's largest digital identity framework, Access Now, https://www.accessnow.org/supreme-court-of-india-rules-to-restrict-worlds-largest-digital-identity-framework-aadhaar-but-debate-continues/
[2] 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

vulnerabilities, and undermine fairness, agency and dignity for people in the digital age.

However, we also acknowledge that context and community sentiment is shifting. Historically, Australians have reacted negatively to proposals for digital identification or centralised identity-related systems, including the rejection of the Australia Card and the high opt-out rate of the MyHealthRecord scheme.

However, following the large-scale data breaches of 2022, the landscape is changing, with more people questioning the safety and security of having so many individual companies and government agencies require the collection of identity documents in order to access and use their services. A well-functioning, robustly safeguarded and carefully implemented government-led digital identity system has the potential to minimise the risks associated with billions of people being compelled to repeatedly hand over their identity documents.

In Europe, many countries have established digital identity structures, however these systems are built on a robust rights-based framework and a mature rights-respecting culture that we do not currently enjoy in Australia.

Digital Rights Watch recognises the potential benefits associated with the establishment of a digital identity system, however we will continue to advocate for a handful of key components that we believe are fundamental for a robust, fair, trustworthy and successful Digital ID system.

The Digital ID system must:

- never be repurposed for surveillance or law enforcement purposes;
- be based on a rights-based framework;
- have robust privacy and digital security protections built in;
- take a decentralised approach;
- be genuinely voluntary, with practical non-digital alternatives available;
- prioritise accessibility, interoperability and inclusivity;
- work for First Nations people and non-Eurocentric models of a person's identity;
- provide actionable pathways for redress where harm or misuse occurs;
- include meaningful accountability, oversight, audit and review mechanisms.

We strongly suggest that the Digital Identity Taskforce continue to engage with civil society and community groups as the process of developing and implementing Australia's digital identity system progresses.

Need for meaningful consultation to build trust

While Digital Rights Watch is eager to participate in digital identity consultations to provide a digital rights civil society perspective, we do note that the extremely short timeframe of three weeks does not allow for genuine input from, or engagement with, many civil society and community concerns. While we appreciate the urgency that the Taskforce may feel, such a short time frame is not adequate for many organisations and individuals to meaningfully participate.

In this short timeframe, the *Identity Verification Services Bill 2023* has also been available for public consultation. The legislative framework proposed in the IVS Bill must be consistent with the Digital ID Bill. These systems are inextricably linked, and will inevitably end up complementing (or contradicting) each other. The current inconsistencies between them risk the creation of loopholes and ineffective governance processes. In particular, we note that the Digital ID Bill proposes markedly more robust privacy protections than the IVS Bill.

These pieces of legislation stand to impact all Australians, and come with significant risks that must be addressed. Short, concurrent consultation periods that do not enable meaningful public contribution undermine public trust. We strongly urge the Government to proceed in a more deliberate, considered way that ensures consistent and harmonious operation between the IVS Bill, the proposed Digital ID legislation, and Australian privacy law with appropriate regard to developing and maintaining public trust.

Reform of the Privacy Act must be prioritised

While we welcome the intention to ensure that accredited entities must be subject to some form of privacy law—be it the Commonwealth *Privacy Act 1988* or a state or territory equivalent—we remain concerned that this is occurring at a time when the Government itself has publicly acknowledged that Australia's existing privacy legislation is nowhere near robust enough to deal with the realities of the modern digital economy, and while many key parts of this legislation are under review.

The current deficiencies in Australia's privacy law leave a number of privacy risks unaddressed. As privacy is a core part of making the Australian Government Digital Identity System (AGDIS) scheme work safely and effectively, we **strongly urge that reform of the Privacy Act be completed *before* extending the Digital ID system beyond its current state.**

We appreciate that legislation is required in order to expand and regulate the AGDIS, to ensure that the Accreditation Scheme meets community expectations, and to create civil penalties otherwise out of reach of the Trusted Digital Identity Framework. However, it is our view that essential reforms to Australia's Privacy Act should be prioritised *before* any expansion of the AGDIS.

Biometric data

The severity of consequences should individuals' biometric data be compromised or misused cannot be understated. As such, Digital Rights Watch has previously expressed concern regarding the integration of biometric data into digital identity systems.

However, Digital Rights Watch is pleased to note the prohibition of collection, use and disclosure of biometric information for the purposes of *one-to-many* matching under section 45. This is an important prohibition to safeguard against the harms associated with *one-to-many* matching.

According to the OAIC's 2023 Community Attitudes Survey, only 49% of Australians are comfortable with the use of their biometric information to verify their identity online.[3]

We also welcome the requirement for accredited identity service providers to immediately destroy biometric information it has collected from an individual for the purpose of verifying that individual's identity after the verification is complete under section 48. This is an important protection measure against potential misuse, over-collection, or unreasonable retention of biometric data. We are of the view that the exemptions to this under subsections (3) and (4) are reasonable.

We note that the bill provides for the Minister to make certain rules to allow the disclosure of biometric information when consented to by the individual. We remain concerned about the use of consent as the only criteria for such regimes. Indeed, this is a motivating concern of the current review of the Privacy Act. We would only consider such a regime to be appropriate where additional and more onerous protections apply, including a fair and reasonable requirement and an obligation placed upon accredited entities that the sharing of a biometric credential be in the best interests of the individual.

Pathways for redress

Given that Australia's Digital ID system relies heavily on the collection, use and disclosure of an individual's biometric data as well as other personal and sensitive information, the risks to an individual's privacy, security, safety and wellbeing should the system suffer a security breach or other forms of misuse are immense. The use of biometric data is particularly dangerous, as generally speaking people cannot readily change their biometric data, making it exceptionally difficult to remedy in the case of a data breach.

[3] The Office of the Australian Information Commissioner, Community Attitudes to Privacy Survey, 2023. https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023

We note that the Guide states:

> *"The Bill will not initially provide specific financial or non-financial redress obligations on accredited entities participating in the AGDIS, or on the Regulator. The Bill will allow the Minister to provide a redress framework in the Digital ID rules."*

It is our view that this does not go nearly far enough to ensure that adequate or effective mechanisms for remedying violations are in place, such that individuals can seek remedies for harms suffered, and access relevant information concerning complaints processes and conciliation processes. Section 83, for example, does not reference compensation or civil penalties payable to affected individuals, which would be appropriate. We also note that the current draft of the Digital ID Rules do not include any reference to a redress framework.

Even the most highly safeguarded systems will likely see problems—including human rights issues—arise. It is essential that an effective redress framework is built into Australia's Digital ID system. At the very least, the provision *allowing* for the Minister to provide a redress framework ought to be amended to *require* the development of a redress framework within a certain, limited timeframe.

Sharing digital ID information with law enforcement

While we appreciate that the Digital ID bill seeks to narrow the scope of disclosure to law enforcement that is permissible in the Privacy Act, **we strongly oppose any repurposing of Digital ID data or infrastructure for surveillance purposes.** No justification has been put forward for allowing such access.

Individuals ought to be able to voluntarily use a Digital ID without any concern that doing so may later be used to enable mass surveillance. Such concerns undermine public trust in these systems. Prohibiting the use of Digital ID data from law enforcement purposes is the most effective way to prevent this from occurring. We recommend that law enforcement agencies should be explicitly prohibited from accessing Digital ID data held by any accredited entities.

Penalties and compliance

Digital Rights Watch is pleased to note that failure to comply with obligations set out under the Bill can lead to compliance action or civil penalties. Civil penalties are an important incentive mechanism to ensure that participating entities take their obligations—especially privacy and security—seriously.

We note that the proposed penalties sit at 200 or 300 penalty units, depending on the conduct. As noted in the table on page 33 of the guide, this translates to a maximum penalty of $469,500 for a corporate or government entity.

Digital Rights Watch is concerned that these penalties are relatively low compared to those under the Privacy Act and Australian consumer law. Given the potential for serious harm to individuals should accredited entities breach their obligations under the Bill, we suggest that the Digital ID Taskforce raise the maximum penalties to better reflect the gravity of collecting and handling individuals' personal and sensitive information, and the severity of harm that can be cause where these systems are breached or misused. The Digital ID Taskforce may wish to consider a tiered penalty regime as proposed in the review of the Privacy Act.

We would also be interested in improvements to transparency around non-compliance and reporting for accredited entities. These could be easily incorporated into the register (s 117) and annual reporting requirements (s 144) currently provided for under exposure draft.

Deactivation and deletion

We welcome the inclusion of section 28 which requires that Digital IDs must be deactivated upon the request of an individual as soon as practicable after the request. There is, however, no clear requirement to also delete or destroy any personal information that the entity may hold in relation to that person's deactivated digital ID. We suggest that the Digital ID Taskforce revisit this section to clarify the retention and deletion requirements upon the entity.

While we appreciate that accredited entities would be required to meet deletion requirements under the relevant privacy legislation (where it exists), we remain concerned that this does not go far enough to prevent entities from retaining personal and sensitive information for longer than they need it.

For example, Australian Privacy Principle (APP) 11.2 requires APP entities to take reasonable steps to destroy personal information or ensure it is de-identified if it no longer needs the information for any purpose.[4] However, this is a loose requirement, as it is possible to argue that a company *needs* to retain personal information for all kinds of purposes. This principle routinely appears to be ignored or misinterpreted, as organisations are regularly retaining personal information far longer than that which is necessary.

For example, following the Optus data breach, customers were outraged to discover their information had been retained for many years, even long after they were no longer an Optus customer. Optus claimed that they were legally-required to retain it for 6 years, although it was never clear which law they were referring to. By retaining so much information for unreasonably long periods of time, entities increase the potential consequences of a data breach.

[4] See APP 11 on Security https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information

With all this in mind, Digital Rights Watch strongly suggests that the Digital ID Bill or the Rules include specific data retention limitations.

Prohibition on data profiling and tracking

Digital Rights Watch welcomes the prohibition on accredited entities using or disclosing information about an individual's online activities, such as the individual's access and use of the Digital ID services provided by the entity, regardless of consent. We note that subsection (3) provides exemptions to this prohibition, including for "purposes relating to the provision the entity's accredited services (including improving the performance or usability of the entity's information technology systems through which those services are provided)". We are somewhat concerned that this provision may allow scope for companies to use information collected or otherwise accessed through the Digital ID system for their own benefit, such as in order to personalise services and generate further revenue, despite that information not being collected for that purpose. We suggest that this provision ought to be tightened.

It is extremely important that individuals are able to use their Digital ID to access services without the fear of their online behaviour being tracked or logged, or tied back to their Digital ID. Many people would rightly be concerned at the prospect of the participating parties or any government body having visibility over all the services or products that they are accessing via the use of their Digital ID. As such, it is essential that clear, preventative steps are in place to safeguard against any potential ability to track, log or aggregate people's activities through the use of their Digital ID.

Section 50(3)(c) provides an exemption to the prohibition on data profiling to track online behaviour if the use or disclosure if required or authorised under a law of the Commonwealth, a State or Territory. It remains unclear to us in what circumstances such disclosure would be required, and whether this includes disclosure pursuant to a warrant obtained by law enforcement. We reiterate comments made above: individuals ought to be able to voluntarily use a Digital ID without any concern that doing so may later be used to enable mass surveillance. Such concerns undermine public trust in these systems.

Digital ID must remain truly voluntary

Digital Rights Watch is pleased to note the emphasis placed on ensuring that creating and using a Digital ID is voluntary in section 71 of the exposure draft. It is clear that there will be a significant portion of the Australian population for whom a digital ID service will be difficult or undesirable to use. It is imperative that there are genuine alternatives to the Digital ID system for those Australians who are unable to use it.

We do note, however, that some of the potential rationales for an exemption to the requirement for access to be voluntary may exacerbate pre-existing

inequalities such as digital exclusion. For example, subsection (5) lists instances where the Digital ID Regulator may be satisfied that it is appropriate to grant an exemption, including if "the participating relying party is providing services, or access to services, in exceptional circumstances." The corresponding Guidance document notes that such exceptional circumstances might include instances such as a natural disaster.

While we appreciate the need for some level of flexibility, we remain concerned that instances where Digital ID is effectively mandatory will essentially cut off a proportion of the population from accessing those services. This, as indicated in the legislation, may be appropriate or manageable where there are adequate alternatives (which may be the case in the private market), however we wish to emphasise that emergency response services such as those in the event of a natural disaster must be made available to *everyone* who needs them, and care must be taken to ensure that the digital divide is not exacerbated in these instances.

Interoperability

Digital Rights Watch welcomes the intention to ensure interoperability between services, to ensure they work efficiently together and to give individuals the freedom to choose which participating accredited Digital ID provider and their Digital ID to be able to access services.

We do note that s 75(3)(c)(iv) allows the Minister to grant an exemption from the interoperability obligation if "an entity will provide an arrangement to assist individuals who would otherwise be at a disadvantage in accessing the Australian Government Digital ID System." We are somewhat concerned that such an exemption may result in the unintended consequence of limiting the choice and data control of people with additional needs. Preferably, all accredited entities should be meeting accessibility and inclusivity requirements and standards to ensure equity and fairness across the Digital ID ecosystem.

In any case, it is not clear to us how reducing interoperability is a solution to ensuring that individuals who may be at a disadvantage in accessing the AGDIS. We suggest further consideration and clarification of this subclause.

Fees

We note that the legislation is currently unclear as to whether it allows accredited entities in the private sector to charge fees in relation to the creation or use of a Digital ID. We do note that the Guide indicates that "the Bill precludes rules being made that would charge an individual a fee to create a Digital ID to use in the AGDIS", recognising that it is inappropriate for Commonwealth entities to charge individuals a fee to access taxpayer funded services. We are concerned that should there be different rules for public versus private entities, this may lead to consumer confusion, disadvantage people who may not be able to afford the fees,

and discourage Digital ID adoption. We believe this section would benefit from further consideration and clarification in the next iteration of drafting.

Specifically, we recommend prohibiting *any* entity from charging a fee for individuals to create or use a Digital ID. Given that the intention appears to be for individuals to use any participating accredited Digital ID provider for access across services, it would create circumstances where people are by default pushed towards using providers that do not charge a fee.

Unintentional collection of sensitive information

Digital Rights Watch welcomes the requirement that accredited entities must be subject to the Privacy Act, or the relevant equivalent state or territory privacy law, as well as the notifiable data breach scheme.

We welcome the prohibition upon intentional collection of certain attributes including racial or ethnic origin, religious beliefs, or sexual orientation under s 41. However, we do wish to emphasise that it is possible to *infer* this information from other, seemingly benign data points. While DRW appreciates that effort has been made to allow flexibility for *unintentional* collection of such information, for example, where a person's facial image indicates religious belief, we remain concerned that there is room for this to create risk of harm. While we agree that unintentional collection should not be prohibited to the extent that it would prevent the scheme from functioning, we do believe there should be additional considerations given to the protection of such information from misuse in instances where it has been unintentionally collected. For example, through requirements to delete the information once it is realised that it is sensitive, or with restrictions that prevent entities from using information they collect to infer sensitive information.