Submission to the Senate Legal Constitutional Affairs Committee

regarding the

Identity Verification Services Bill 2023

02 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

General remarks

Digital Rights Watch welcomes the opportunity to provide comments to the Senate Legal Constitutional Affairs Committee regarding the *Identity Verification Services Bill 2023* ('the IVS Bill').

We do note, however, that the extremely short amount of time provided for public consultation of less than three weeks does not allow for genuine input from, or engagement with, civil society and community concerns. While we appreciate the urgency that Parliament may feel to action this legislation, such a short time frame is not adequate for many organisations and individuals to participate.

Further, we note that the IVS Bill seeks to instate a legislative framework for processes that *are already in practice*. It is our view that it is entirely inappropriate for these practices to have been occurring for so long, without a legislative authority to do so. We understand that this may be a motivating factor for the Government to proceed urgently with the IVS Bill. However, the nature of the IVS Bill as an instance of retrofitting a legislative foundation to an existing set of practices, combined with the extremely short timeframe for public review and feedback, brings the meaningfulness of this consultation into question.

In this short timeframe, the exposure draft of the Digital ID Bill 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. 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, and as a bare minimum, the IVS Bill ought to be amended to match the privacy protections proposed under the Digital ID framework.

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. This is made worse given the circumstances in which the previous iteration of the Bill was rejected for an absence of proper rights protections, and yet the underlying practices carried on without a legislative basis notwithstanding.

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 and privacy protections strengthened

While we welcome the intention to ensure that parties to IVS agreements will be subject to some form of privacy law, there are many parts of the IVS Bill that allude to a patchwork of privacy protections in minimal detail. This comes 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 in the IVS Bill. As privacy is a core part of making this scheme work safely, we **strongly urge that reform of the Privacy Act be completed *before* such potentially pivotal systems such as IVS are built on top of its guarantees.**

Alternatively, the Government should amend the IVS Bill to insert additional privacy protections consistent with those included in the exposure draft of the *Digital ID Bil 2023*. As emphasised above, these two schemes must be harmonious. It is unreasonable for people's privacy to be undermined by the less effective privacy law protections in the IVS Bill.

Relatedly, we note that the IVS Bill requires parties to comply with standards set by the *Privacy Act 1988* or similar State or Territory laws. It is our view that this flexibility enables participating parties to opt for the lowest applicable privacy protections. Instead, participation should be predicated upon compliance with strongest possible privacy protections in Australia and as such require compliance with the Australian Privacy Principles under the Privacy Act as a bare minimum.

Detection of and penalties for misuse

Digital Rights Watch is pleased to note the requirement for annual audits of all IVS participants (by which we take to mean any entity that is party to a "participation agreement" including both government and non government entities, as well as any contracted service providers), as detailed in Clause 12 of the Bill.

However, we note that audits of this nature are only valuable for detecting instances of misuse *after* they have already occurred, rather than acting as a meaningful, preventative measure. On its own, auditing is not a sufficient detection mechanism for the potential misuse of something as important as the IVS. In addition to the proposed auditing program, Digital Rights Watch recommends the adoption of more proactive misuse detection measures for IVS participants, including meaningful monitoring and alerting on third-party IVS access; granular, role-based access control mechanisms; and service rate limiting where appropriate and practical.

We note that a party's ability to make use of the verification services can be suspended or terminated if they have not complied with the agreement or access policies of the service. While this is a positive and necessary step, we do not believe it to be a strong enough deterrent from misuse of the identification services, particularly if this is expected to act as the *only* deterrent mechanism, which is all that is currently provided for in the Bill:

> *While the Bill does not provide civil penalties for non-compliance with a participation agreement, the potential impact of a suspension or termination may be severe and is expected to act as a deterrent against non-compliance.*[1]

An absence of explicit civil penalties or criminal offences in the IVS Bill for participating entities, including the Department, is woefully inadequate. By way of contrast, the Attorney General has recognised that the current civil penalties available in the Privacy Act are inadequate, and is on the record as being committed to expanding enforcement powers under the Privacy Act, including both civil penalty provisions and applications for relief made directly by individuals. An approach that favours even fewer enforcement powers, in the context of a regime that deals with very sensitive information, is inappropriate.

As demonstrated during and following the large-scale data breaches of 2022, robust penalties create a powerful incentive for businesses to adhere to laws regarding the security of personal information. We do note that in limited circumstances the civil penalty provisions under section 13G of the Privacy Act would apply, however this provision only applies to APP entities, and therefore would not cover all participating entities in the IVS scheme. **As such, Digital Rights Watch recommends implementation of robust penalties for participants that misuse the IVS system.**

We further note that there is currently no obligation to notify anyone who might be affected by non-compliance. We suggest that such a provision for notification ought to be included in the IVS Bill.

There also does not appear to be any meaningful consequence for inappropriate *use* of protected information. While section 10(1)(c) prohibits parties from using the outcome of an IVS as the only evidence of the individuals' identity in criminal or civil proceedings, inappropriate *use* of the outcome is not captured by the offences set out in section 30, which lists only recording, disclosing or accessing information. This ought to be extended to capture inappropriate or unreasonable use of protected information, including the outcome of the IVS.

Finally, the IVS Bill relies primarily upon the mechanisms for individual redress and systemic oversight contained in the Privacy Act as well as corresponding state, territory and New Zealand privacy legislation. Given the shortcomings of the

[1] Point 199 of the IVS Bill Explanatory Memorandum

pathways for redress under the current Privacy Act, we strongly recommend the IVS Bill be amended to provide the OAIC with additional powers and resources to manage a more comprehensive redress mechanism for individuals affected by the operation of the IVS scheme. Again, finalising reform of the Privacy Act *before* continuing with the IVS Bill is preferable.

Such a redress mechanism should allow an individual to submit complaints about the handling of their identification information by either the Department, or a party to a participation agreement or the NDLFRS hosting agreement, and include appropriate measures to remedy any harm suffered by the individual.

Clarification of "consent"

Much of the IVS Bill is dependent on the concept of "consent." For example, section 35(1) includes a carve out that permits an entrusted person to make a record of, disclose or access protected information "if the person has consented." We further note that point 356 of the Explanatory Memorandum says: *"The concept of 'consent' in the Bill is intended to include express consent or implied consent."*

Digital Rights Watch remains concerned that such a provision could be subject to misuse where individuals may not be in a position to meaningfully refuse if an entrusted person compels them to provide consent, or where "implied" consent is unreasonably applied. We urge the Government to consider the addition of a fair and reasonable test, in line with the proposal contained in the Privacy Act Review.

Facial recognition is dangerous

The current version of the IVS Bill addresses some of the criticisms related to privacy and transparency which led to the failure of the previous iteration of the Bill, the *Identity Matching Services Bill 2019.* At the time, there were widespread and justified concerns that the 2019 Bill would enable mass surveillance of Australians through the use of 1:many face matching (also referred to in the Bill as the Facial Identification Service (FIS)).

We are pleased to note that the use of 1:many matching has been considerably limited in the current version of the Bill, with section 17 restricting FIS use to a subset of law enforcement in cases directly involving the protection of shielded persons, such as those in a witness protection program. Although this significantly reduces the situations in which 1:many face matching technology may be used, this Bill does not outlaw the technology, leaving space for these capabilities to be further developed. 1:many facial surveillance systems are fundamentally incompatible with a rights-respecting liberal democracy.

We recommend including additional restrictions on the use of 1:many technologies and their development, to prevent the expansion of these capabilities by the Australian Government for use in these circumstances or

potential future applications. In our view, this could be done by including a requirement that the use or access to the FIS be permitted only when the relevant authority has sought a court authorisation, in addition to the conditions set out in the bill. The court could consider the basis for the request, and balance this with any concerns around cybersecurity and privacy, with a confidentiality regime in place in recognition of the sensitive subject matter. This process of independent review of applications to access the FIS would reflect the serious nature of the information being sought and protect against scope creep.

Public scrutiny of facial recognition systems

We note the provision in section 41 for annual reporting on "information about the accuracy of the systems for biometric comparison of facial images that are operated by the Department". While it is useful that the Government considers this an important point to measure, we note that this is a self-reporting mechanism which only provides data after inaccuracies have occurred.

There is long precedent to demonstrate that the biases in the data used to train machine learning models will be present in the results output by the model in active use. In many cases, where these models are used in facial recognition or matching systems, these biases result in false matches being returned for people of colour, minority genders, and children. This presents a risk to members of these already marginalised populations, regardless of whether the technology is used in 1:1 or 1:many contexts, and has led to cases of wrongful accusation and detention across the world.

Given the potential severity of such impacts, and the fact that these systems are intended to be used upon the Australian public, we strongly recommend that all system implementation details, machine learning models, and associated training input used by the Australian Government in the provision of both 1:1 and 1:many face matching services be made available to the Australian public and independent experts for scrutiny and transparent, proactive reporting on the performance and accuracy of such systems.

Robust digital security is essential

We note that section 25 includes a requirements that the Department must:

> *(a) maintain the security of electronic communications to and from the facility, including by encrypting the information; and*
>
> *(b) protect the information from unauthorised interference or unauthorised access.*

However, there is very little in the IVS Bill with regard to:

- how the data will be protected, and whether specific standards will be adhered to,
- what happens if the systems fail to secure the information, and
- who is to be held accountable in the event of a breach and how, including in instances of 'human error' — all provisions for penalties for entrusted persons are based on malicious intent or negligence, not accident.

Further to this, we note that data breaches are not subject to mandatory disclosure, only if the breach is "reasonably likely to result in serious harm to an individual to whom that information relates" under s 9(2) and with respect to the NDLFRS under section 13(4). This condition ought to be removed and mandatory disclosure of data breaches enforced.

Digital Rights Watch notes that the function of this entire system relies upon robust encryption for protection. As such, any other legislative or policy efforts to reduce the effectiveness of encryption technologies for other reasons (for example, with regard to online safety and law enforcement purposes) should be abandoned. Any permitted weaknesses in encryption technologies creates the potential for detrimental impacts on the IVS and the valuable data that it holds on Australians. It is not possible to weaken encryption for one purpose, and rely on it for another.

Recommendations

1. Review and amend the drafting of the IVS Bill as a whole to more clearly articulate the IVS scheme and its operation, with a focus on upholding the rights of individuals and clarifying the responsibilities of participating entities and entrusted persons.
2. Prioritise robust reform to the *Privacy Act 1988 before* the IVS Bill.
    a. Alternatively, amend the IVS Bill to insert additional privacy protections consistent with those included in the exposure draft of the *Digital ID Bil 2023*.
3. Increase the privacy requirements to meet the standards contained within the (reformed) *Privacy Act 1988* as the minimum acceptable standard.
4. In addition to the proposed auditing program, adopt more proactive misuse detection measures for IVS participants, including meaningful monitoring and alerting on third-party IVS access; granular, role-based

access control; and service rate limiting where appropriate and practical.

5. Implement a penalty scheme for participants that misuse the IVS system, including the Department. Include a provision requiring the notification of individuals in instances where they are affected by non-compliance.

6. Include a penalty for inappropriate use or application of an IVS outcome by an entrusted person in addition to recording, accessing or disclosing protected information.

7. Provide the OAIC with additional powers and resources to manage a more comprehensive redress mechanism for individuals affected by the operation of the IVS scheme.

8. Include a requirement that the use or access to the FIS be permitted only when the relevant authority has sought a court authorisation, in addition to the conditions set out in the Bill.

9. Consider the addition of a fair and reasonable test, rather than reliance on implied consent, in line with the proposal contained in the Privacy Act Review.

10. Amend Clause 43 to provide for an interim review of the operation of the IVS scheme after 12 months, focusing on adequacy of the privacy protections. We also suggest that subclause 44(4) be amended to shorten the sunset clause.

11. Remove the limiting condition upon mandatory disclosure under section 13(4) and ensure that all data breaches of the IVS are subject to mandatory notification.

12. Abandon any and all proposals that seek to undermine, weaken or in any way act to the detriment of encryption technologies.