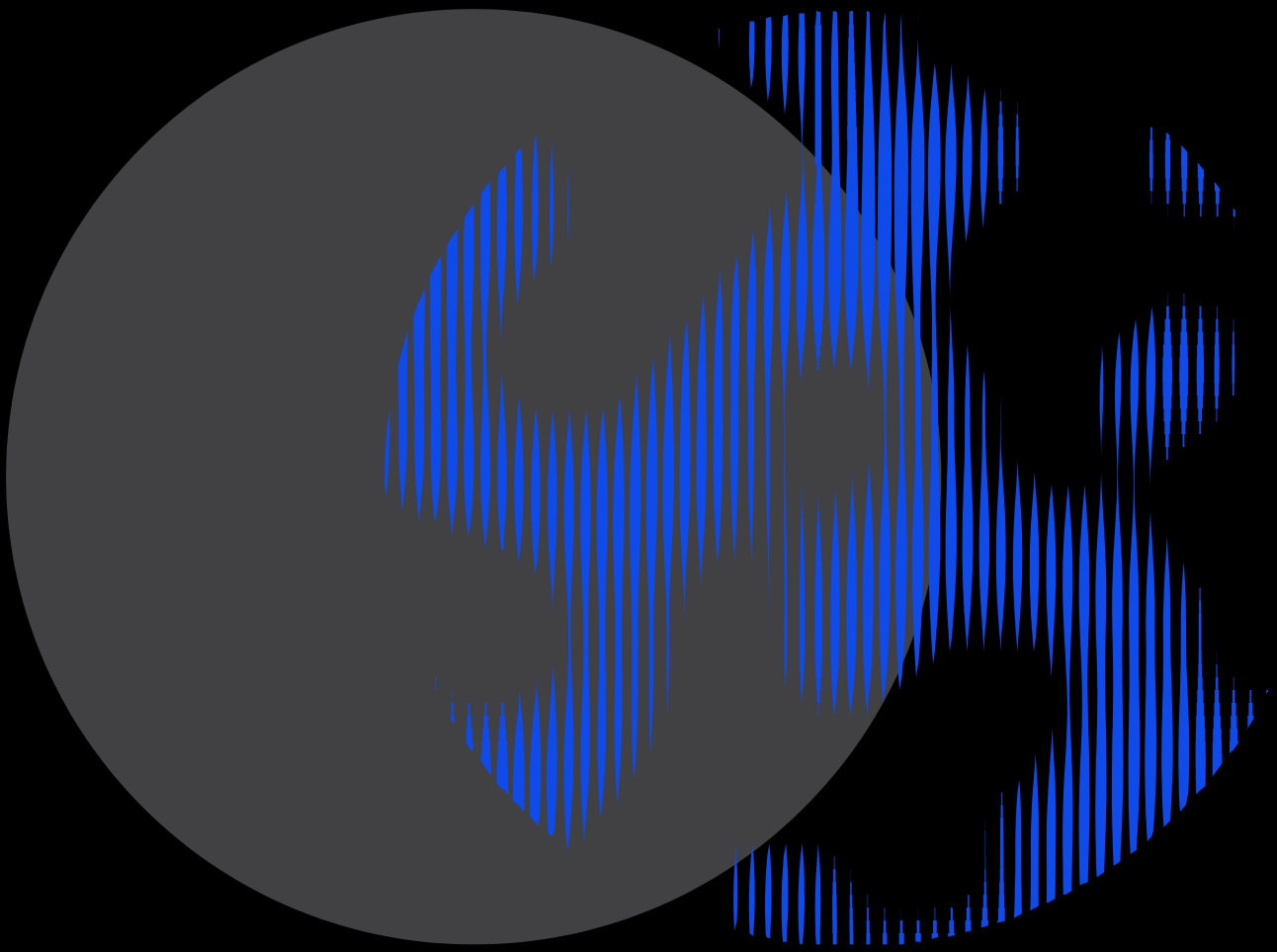
Human Technology Institute



Submission to the Legal and Constitutional Affairs Legislation Committee inquiry into the Identity Verification Services Bill 2023 and the Identity Verification Services (Consequential Amendments) Bill 2023

Human Technology Institute, UTS

29 September 2023

29 September 2023

About the Human Technology Institute

The Human Technology Institute (HTI) is building a future that applies human values to new technology. HTI embodies the strategic vision of the University of Technology Sydney (UTS) to be a leading public university of technology, recognised for its global impact specifically in the responsible development, use and regulation of technology. HTI is an authoritative voice in Australia and internationally on human-centred technology. HTI works with communities and organisations to develop skills, tools and policy that ensure new and emerging technologies are safe, fair and inclusive and do not replicate and entrench existing inequalities.

The work of HTI is informed by a multi-disciplinary approach with expertise in data science, law and governance, policy and human rights.

In this submission, HTI draws on several of its major projects, including:

Facial Recognition Technology: Towards a model law. In a world-leading report published in September 2022, HTI outlined a model law to govern facial recognition technology in Australia.

AI Corporate Governance Program, which is aiming to broaden the understanding of corporate accountability and governance in the development and use of AI.

The Future of AI Regulation in Australia, which is considering the major legal and policy issues related to AI and will present a roadmap for reform.

For more information, contact us at hti@uts.edu.au

Acknowledgement of Country
UTS acknowledges the Gadigal people of the Eora Nation, the Boorooberongal people of the Dharug Nation, the Bidiagal people and the Gamaygal people upon whose ancestral lands our university stands. We would also like to pay respect to the Elders both past and present, acknowledging them as the traditional custodians of knowledge for these lands.

Authors: Professor Edward Santow and Sophie Farthing

HTI acknowledges the contribution and support of India Monaghan, Secondee – HTI Policy.

To discuss this submission, please contact us at hti@uts.edu.au.

29 September 2023

Table of contents

29 September 2023

Executive summary

The Human Technology Institutes (**HTI**) welcomes the opportunity to comment on the Identity Verification Services Bill 2023 (Cth) (the **IVS Bill**), and the accompanying consequential amendments bill.

The IVS Bill would provide legislative authority for a range of government identity verification services. As discussed below, these services are already in operation without any apparent legislative foundation. This may be a motivating factor in the Australian Government (**Government**) deciding to proceed urgently with the IVS Bill. An unfortunate consequence of that urgency is that there is very limited scope for public consultation on a major reform that affects Australians' right to privacy, among other rights.

In addition, the Government has also published exposure draft legislation in respect of digital identity, and announced its response to the Attorney-General's Department review of Australia's privacy legislation. These three reform processes are inextricably linked. That fact, coupled with the curtailed opportunity for public consultation, means that it would be far preferable for the Government to proceed in a more deliberate way – by enabling more extensive public consultation, and ensuring consistent and harmonious operation between the IVS Bill, proposed digital identity legislation and Australian privacy legislation.

On the substance of the IVS Bill, HTI acknowledges a number of positive elements. In particular, it is important that a major scheme such as this be regulated by clear primary legislation. In addition to enabling a range of activities, the IVS Bill provides three defences against the risk of harm to individuals:

- the Bill contains privacy protections
- the Bill limits the use of 1:many facial recognition technology in respect of data within the ambit of the Bill itself
- the Bill provides for some forms of individual redress, systemic oversight and review.

While these defences are important, they are also limited. HTI recommends changes that would improve each of the defences in the IVS Bill.

Privacy protections

The IVS Bill relies largely on the protections in the *Privacy Act 1988* (Cth) (**Privacy Act**), or corresponding state, territory or New Zealand legislation, to ensure that individuals' privacy rights are upheld. However, there are a number of deficiencies with this existing privacy legislation, as the Government itself recognised through the Attorney-General's Department (**Department**) 2022 Privacy Act review and its official response to that review on 28 September 2023.

Those deficiencies leave a number of privacy risks inadequately addressed in the IVS Bill. There would be three ways of addressing that problem.

First, the Government could simply amend the Privacy Act – implementing the relevant recommendations from the Attorney-General's Department review – prior to the passage of the current IVS Bill. This would be the most logical and simplest way of uplifting the relevant privacy law protections.

Secondly, the Government could amend the IVS Bill by inserting similar additional privacy protections to those included in the Government's exposure draft Digital ID Bill 2023. This would have the benefit of ensuring those closely-related schemes would be harmonious, and would not be undermined by the less effective privacy law protections in the IVS Bill.

Thirdly, the Government could amend the rule-making power in cl 44 of the IVS Bill to enable the Minister to introduce stronger privacy protections in line with the exposure draft Digital ID Bill 2023 – at least until either of the above two amendments to primary legislation have been achieved.

1:many facial recognition technology

HTI endorses the IVS Bill's strict limitations in respect of the use of 1:many facial recognition technology within the scope of the IVS Bill itself.

However, the Bill does not seek to regulate the rising use of 1:many facial recognition through a range of commercial and other services. Many such services carry very significant risks to the right to privacy, with limited protection from the current Privacy Act. The Government is committed to addressing the risks associated with 1:many facial recognition technology in the context of reform on digital identity – of which this Bill is a crucial part. HTI urges this Committee to recommend that this reform take place, using HTI's model law for facial recognition technology as the guide.

Individual redress, systemic oversight and review

The Bill relies primarily on the mechanisms for individual redress and systemic oversight contained in the Privacy Act, as well as corresponding state, territory or New Zealand legislation. This submission sets out a number of ways in which the redress and oversight regime should be improved, taking into account the exposure draft Digital ID Bill 2023.

The Bill also provides for a statutory review after two years' operation. Given the need for additional transitional arrangements to protect the right to privacy, HTI recommends an interim review after one year of operation.

List of recommendations in this submission

Recommendation 1: HTI recommends that the privacy protections in the IVS Bill be strengthened to make them at least consistent with the Government's exposure draft Digital ID Bill 2023. This could be achieved in any of the following ways, set out below in order of HTI's preference:

(a) amend the Privacy Act in a way that implements the relevant recommendations from the AGD Privacy Review 2022, prior to the passage of the IVS Bill
(b) amend the IVS Bill to include additional privacy protections, substantially mirroring the relevant additional privacy protections in Chapter 3 of the exposure draft Digital ID Bill 2023
(c) amend cl 44 of the IVS Bill to empower the Minister to make rules to strengthen the privacy protections in the IVS Bill, with a sunset clause applicable to the IVS Bill as a whole, if the Minister fails to enact such rules within a specified period (eg, six months).

Recommendation 2: HTI recommends that cl 44 of the IVS Bill be amended to provide for consultation with the public, and the Information Commissioner, in a manner similar to cl 159 of the Digital ID Bill 2023.

Recommendation 3: HTI recommends that the Government introduce legislation to regulate all forms of facial recognition technology, by implementing the Human Technology Institute's FRT model law.

Recommendation 4: HTI recommends that the IVS Bill impose civil penalties or criminal offences in relation to the misuse of the identity verification services and identification information obtained through the identity verification services.

Recommendation 5: HTI recommends that 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. Such 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.

Recommendation 6: HTI recommends that the IVS Bill and Privacy Act be amended to provide the Information Commissioner with greater powers and independence in relation to their assessment function, including by:

(a) inserting a new provision in s 33C of the Privacy Act to allow the Information Commissioner to conduct an assessment of the operation and management of the IVS scheme and IVS Bill, which may be conducted in such manner as the Information Commissioner sees fit

(b) inserting a provision similar to cl 40 of the Digital ID Bill 2023 to provide the Information Commissioner with an advisory role in relation to the operation of the Bill at the request of the Minister.

Recommendation 7: HTI recommends that the drafting of the IVS Bill as a whole be reviewed and amended to more clearly and effectively describe the IVS scheme, its operation and the rights and responsibilities of individuals and participating entities to ensure easier interpretation of the IVS Bill.

Recommendation 8: HTI recommends that:

(a) "facial recognition and image comparison", and the training requirements in relation to this activity, be specified in the relevant participation agreements or access policies for FVS and FIS

(b) all Department officers, members of staff, employees, contractors and employees of contractors who handle facial images in relation to a request for FVS or FIS be required to undertake the same facial recognition and image comparison training that persons receiving images undertake.

Recommendation 9: HTI recommends that cl 43 of the IVS Bill be amended to provide for an interim review of the operation of this law after 12 months. That interim review should focus on the adequacy of the privacy protections operating in the IVS scheme.

Background

Prior to the IVS Bill, the then Home Affairs Minister introduced two previous bills, the main one being the Identity-matching Services Bill 2019 (Cth) (**IMS Bill**). Those Bills would have had the effect of establishing a legal regime for the services covered by the current IVS Bill, as well as a range of other services.

The Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) conducted a review into the IMS Bill. There was widespread expert and community concern about the inadequacy of privacy and other protections in the IMS Bill. Ultimately, the PJCIS unanimously recommended that the IMS Bill be withdrawn and substantially redrafted to address such concerns.[1] The Government took the extraordinary step of proceeding with many of the activities contemplated by the 2019 IMS Bill (the **IVS scheme**), despite the fact that the IMS Bill, which had been intended to provide a legislative foundation for this scheme, did not proceed.

In other words, the Government has been operating a number of identity verification services – including the Document Verification Service, Face Verification Service and Face Identification Service – without any obvious legislative authority. The IVS scheme is significant by any measure. As the Explanatory Memorandum to the IVS Bill observes: “In 2022, the DVS was used over 140 million times by approximately 2700 government and industry sector organisations, and there were approximately 2.6 million FVS transactions in the 2022-23 financial year”.[2]

The IVS Bill would provide legislative authority for the operation of the IVS scheme. It does not purport to provide retroactive authorisation for the many millions of transactions that have already taken place, and which are continuing to take place, before the IVS Bill is passed and commences operation. Given the enormity of the IVS scheme and the broad reliance on its lawful operation by thousands of government and other entities, the Government should explain the current legal basis for the IVS scheme.

[1] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory report on the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019* (Report, October 2019).
[2] Explanatory Memorandum, Identity Verification Services Bill 2023 (Cth) and Identity Verification Services (Consequential Amendments) Bill 2023 (Cth) [3].

Issues

Privacy protections in the Bill

The IVS scheme deals with sensitive personal information. As such, there is a need for strong privacy law protections to guard against the misuse or non-consensual use of individuals' personal information, and also to build trust in the IVS scheme. The IVS Bill contains three forms of privacy protection.

The principal mechanism for protecting privacy in the IVS Bill is that it requires IVS scheme participants to comply with the *Privacy Act 1988* (Cth) (**Privacy Act**), or a corresponding state or territory privacy law, the New Zealand *Privacy Act 1993* in relation to New Zealand authorities, persons or bodies, or in the case of some non-government entities, to undertake to comply substantially with the Australian Privacy Principles (**APPs**) in the Privacy Act. The IVS Bill also contains a small number of minor additional privacy protections beyond those set out in the Privacy Act. For example, the IVS Bill requires privacy impact assessments to be undertaken as a requirement for requesting identity verification services.

The IVS Bill also augments the Privacy Act data breach provisions by requiring that *any* breach of security, which relates to a party and is relevant to a matter dealt with in a participation agreement, must be reported to the Department. This expands on the Notifiable Data Breaches scheme (Part IIIC), which only requires that an APP entity notify the Information Commissioner and affected individuals of a data breach where there is unauthorised access to or disclosure of information, *and* it is reasonably likely that such access or disclosure would result in serious harm to any individuals whose personal information was involved in the breach.

Secondly, in order for entities to participate in the IVS scheme, they must be bound by a relevant participation agreement, some of the terms and conditions of which aim to uphold privacy protections. The Bill would provide a legislative foundation for those participation agreements.

Thirdly, the IVS Bill would grant to the Information Commissioner a number of oversight functions. Specifically, under cl 40, the Information Commissioner must annually assess the operation and management of the approved identity verification facilities by way of a written report.

HTI considers that the privacy protections in the IVS Bill are inadequate. The privacy obligations contained in cls 8-12 for participation agreements, and in cl 13 for the NDLFRS hosting agreement, offer minimal additional protections beyond those contained in the Privacy Act. As a result, individuals cannot be certain that their personal information will be protected to the necessary standards, particularly in relation to biometric and other sensitive information.

It is widely acknowledged that the Privacy Act is in urgent need of reform, especially to address the rise of new technologies such as those at the heart of this IVS Bill. The Attorney-General's Department's own 2022 review of the Privacy Act (the **AGD Privacy Review 2022**), as well as other reviews and

inquiries undertaken by government authorities and regulators,[3] highlight problems with the existing Privacy Act and recommend specific amendments. On 28 September 2023, the Attorney-General announced the Government's response to the AGD Privacy Review 2022, indicating an intention to draft legislation that would implement many of the Review's recommendations.[4]

In this context, it is troubling that the IVS Bill does not address the inadequacies in current privacy law, but rather relies primarily on the current Privacy Act to uphold the right to privacy in respect of the IVS scheme. The remainder of this part of the submission sets out a number of options for addressing this problem.

Amending the Privacy Act prior to passing the Bill

HTI's primary position is that it would be preferable to amend the Privacy Act in line with the AGD Privacy Review 2022 recommendations, prior to Parliament proceeding with this IVS Bill. The Government's recent response to the AGD Privacy Review 2022 reflects the Government's intention to strengthen a number of provisions in the Privacy Act. If those Privacy Act amendments were made, this would change the obligations that apply under the IVS Bill.

Nevertheless, Parliament can assess the IVS Bill only by reference to the existing legal protections that the IVS Bill invokes, and those protections are inadequate. It would be reasonable for this Committee to insist that the Government first introduce amendments to the Privacy Act, based on the AGD Privacy Review 2022, prior to recommending the passage of the IVS Bill.

That approach would have two advantages. First, it would improve the privacy protections for the millions of Australians whose personal information is used in the IVS scheme. Secondly, it would provide regulatory certainty for the government and non-government organisations currently participating in the IVS scheme. The alternative approach, whereby Parliament first passes the IVS Bill, then shortly thereafter changes the underlying legal rules in the Privacy Act, would create a significant regulatory burden for the approximately 2700 organisations that already participate in the IVS scheme and those that join it.

While the most logical solution to the privacy problem in the IVS Bill would be to amend the Privacy Act prior to the IVS Bill being passed, it is impossible to ignore the unusual context in which the IVS Bill has been introduced. That is, the IVS Bill seeks to provide legislative authority to the IVS scheme – a scheme that has already been in operation for several years without any specific or obvious legislative authority. It is possible that the Government considers that the urgent passage of the IVS Bill is a necessary expedient, and that any delay caused by proceeding first with broader Privacy Act reform would increase the Government's liability in the event that the IVS scheme is found to be operating unlawfully. If that is the Government's motivation in proceeding so urgently with this IVS Bill, rather than first amending the Privacy Act, it should say so directly

[3] See, eg, 'Digital platform services inquiry 2020-25', *Australian Competition and Consumer Commission* (Web Page) <https://www.accc.gov.au/inquiries-and-consultations/digital-platform-services-inquiry-2020-25>; Australian Human Rights Commission, *Human Rights and Technology* (Final Report, 2021) <https://humanrights.gov.au/our-work/technology-and-human-rights/publications/final-report-human-rights-and-technology>.
[4] Attorney-General's Department, *Government Response: Privacy Act Review Report* (Government Response, 28 September 2023).

– otherwise, there is no obvious reason to proceed with the IVS Bill prior to the Privacy Act reform.

In any case, in the event that the IVS Bill is given priority over broader reform to the Privacy Act, there are two alternative solutions to the inadequate privacy protections in the IVS Bill. These are addressed in turn.

Achieving consistent privacy protections with draft digital ID law

On 19 September 2023, the Government, through the Department of Finance, commenced public consultation on exposure draft legislation on digital identity, in particular the exposure draft Digital ID Bill 2023 (**Digital ID Bill**). That draft legislation would build on the IVS scheme to create a broader and more comprehensive digital identity regime for Australia. In other words, the proposed digital identity scheme is directly connected to the IVS scheme, and it would be both logical and practical for the schemes to operate harmoniously, and subject to consistent legal standards.

However, the Digital ID Bill adopts a different and, in public policy terms, superior approach to privacy protection as compared with the IVS Bill. Essentially, the Digital ID Bill does not rely solely on the Privacy Act protections; instead, Chapter 3 of the Digital ID Bill contains a number of additional provisions that provide stronger privacy safeguards – especially in relation to the protection of sensitive information, including biometric information, and the application of consistent privacy protections to all parties that use digital ID services.

The IVS Bill and the Digital ID Bill are designed to work in tandem, with similar services being provided under each proposed law and similar risks associated with the implementation of such services. HTI recommends that the IVS Bill be amended to include privacy protections that bring the IVS Bill in line with the privacy protections in the Digital ID Bill.

For example, the following provisions in the Digital ID Bill could be adopted also in the IVS Bill:

- *express consent from individuals* – the Digital ID Bill requires that accredited entities obtain *express* consent from individuals in relation to the collection, use, disclosure and subsequent destruction of biometric information (cls 45 and 48) and disclosure of restricted attributes (cl 43). The explanatory memorandum to the IVS Bill (**Explanatory Memorandum**) states that consent, as used within the IVS Bill, includes implied consent,[5] which results in individuals having less control and autonomy over the uses of their personal information for the purposes of the IVS Bill. If the IVS Bill were amended to require participating entities to obtain *express* consent prior to the collection, use and disclosure of biometric and other sensitive information, this would harmonise the two regimes in a way that better upholds the right to privacy
- *monetary penalties for non-compliance* – the Digital ID Bill includes numerous monetary penalties for non-compliance with the provisions,

[5] Explanatory Memorandum, Identity Verification Services Bill 2023 (Cth) and Identity Verification Services (Consequential Amendments) Bill 2023 (Cth) [356].

with penalty-related protections including the destruction of biometric information immediately after verification (cl 48), authorisation or prohibition on handling certain information, and greater protection of restricted attributes (such as health information and unique identifiers assigned to an individual) (cl 43)

- *extended meaning of 'personal information'* (cl 33) – the Digital ID Bill extends the meaning of personal information to include attributes of individuals, which results in information that is associated with an individual and can be derived from another attribute being considered personal information for the purposes of the Digital ID Bill. It is worth noting that this definitional approach to 'personal information' was also recommended in the AGD Privacy Review 2022
- *Privacy Act civil penalty provisions* – in relation to entities that are not subject to the Privacy Act or sufficiently similar privacy legislation, the Digital ID Bill transposes the provisions under ss 13 and 13G of the Privacy Act to apply to non-APP entities that undertake an act or practice that is an interference with privacy of the individual for the purposes of the Privacy Act and imposes the related civil penalties on those entities as if they were APP entities (cls 35 and 36)
- *prohibitions against using information from the IVS scheme* – entities that obtain information through use of the digital ID services are broadly prohibited from using that information for data profiling to track online behaviour (cl 50) and marketing purposes (cl 52). These would be useful protections to add to the IVS Bill.

A possible counter-argument to including bespoke privacy law protections in the IVS Bill, and by extension the Digital ID Bill, is that this would contribute to a fragmentation of privacy law protections. In other words, it would detract from the goal of creating a single source of privacy legislation, at least for the federal jurisdiction. Accepting that there is value in a single legislative approach to privacy, this Committee must weigh up which is the lesser of two evils: a less-fragmented system that provides inadequate privacy protections in a particularly sensitive area of government and commercial activity, or a more fragmented system that provides more effective privacy protections in this area.

HTI strongly advocates for the second of these options. As privacy is a fundamental human right, the problem of fragmentation is less significant than that of inadequate protection. Moreover, given the Digital ID Bill provides for a different set of privacy protections in any event, the risk in leaving the IVS Bill unamended would be the creation of three separate privacy regimes. Harmonising the IVS and Digital ID legislative regimes would reduce this number by one.

Improving the IVS Bill's privacy protections via subordinate legislation

If this Committee accepts the Government's claimed urgency in passing the IVS Bill, there is a further, more expedient way of improving the IVS Bill's privacy protections – namely, to include additional privacy protections in subordinate legislation.

Clause 44 of the IVS Bill already vests a broad rule-making power in the Minister – namely, the Attorney-General. That rule-making power could be expanded to empower the Minister to make rules to strengthen the privacy protections application to the Bill. This would allow the Minister to create subordinate legislation to bring the privacy protections in the IVS Bill at least into line with those in the Digital ID Bill.

If cl 44 of the IVS Bill were amended in this way, it would be wise to include a sunset clause applicable to the IVS Bill as a whole, which would apply only if the Minister fails to introduce the privacy-protective rules within a specified period (eg, six months). Moreover, the IVS Bill could include a provision to the effect that any such privacy rules introduced under cl 44 of the Bill are superseded by privacy protections introduced in due course into the Privacy Act, or the IVS Act when passed.

Additionally, the rule-making power in cl 159 of the Digital ID Bill requires that consultation be undertaken prior to the Minister prescribing any rules. This includes public consultation and consultation with the Information Commissioner for matters that relate to privacy. No equivalent consultation provision exists in cl 44 of the IVS Bill. Yet the IVS Bill deals with substantially similar issues with similar risks, including to the right to privacy. HTI therefore recommends that cl 44 be further amended to include such a consultation requirement.

Recommendation 1: HTI recommends that the privacy protections in the IVS Bill be strengthened to make them at least consistent with the Government's exposure draft Digital ID Bill 2023. This could be achieved in any of the following ways, set out below in order of HTI's preference:

(a) amend the Privacy Act in a way that implements the relevant recommendations from the AGD Privacy Review 2022, prior to the passage of the IVS Bill
(b) amend the IVS Bill to include additional privacy protections, substantially mirroring the relevant additional privacy protections in Chapter 3 of the exposure draft Digital ID Bill 2023
(c) amend cl 44 of the IVS Bill to empower the Minister to make rules to strengthen the privacy protections in the IVS Bill, with a sunset clause applicable to the IVS Bill as a whole, if the Minister fails to enact such rules within a specified period (eg, six months).

Recommendation 2: HTI recommends that cl 44 of the IVS Bill be amended to provide for consultation with the public, and the Information Commissioner, in a manner similar to cl 159 of the Digital ID Bill 2023.

1:many facial recognition technologies

Clauses 16-18 of the IVS Bill deal with the use of the Face Identification Service (**FIS**), which involves 1:many facial recognition technology (**FRT**). These provisions limit the use of the FIS (and, as such, 1:many FRT) in relation to the Face Matching Service Hub to circumstances in which a shielded person's identity must be protected. HTI supports these provisions of the Bill: they

appropriately restrict the extent to which the Bill authorises 1:many FRT being used within the IVS scheme itself.

However, it is important to observe that the IVS Bill only seeks to regulate the use of 1:many FRT via the FIS. It does not purport to regulate other government or non-government uses of 1:many FRT. There is an increasing number of private sector companies offering 1:many FRT services that, on their face, severely restrict the right to privacy without adequate human rights justification. Existing Privacy Act provisions only deal with this scenario in a very limited way, and so this activity is largely unregulated. Both the AGD Privacy Review 2022 and HTI itself have noted that existing federal law does not sufficiently regulate the use of 1:many FRT.

There have been media reports suggesting that the IVS Bill would outlaw most forms of 1:many FRT.[6] This is not the effect of the Bill. However, the need for reform to regulate other forms of 1:many FRT is urgent. The Government's response to the AGD Privacy Review 2022 explicitly acknowledges the need for further reform in respect of facial recognition technology, and it states that "this work should be coordinated with the Government's ongoing work on Digital ID and the National Strategy for Identity Resilience".[7]

The IVS Bill, and the scheme that it seeks to regulate, is fundamental to Australia's digital identity system. Therefore, this Committee should call on the Government to make good on its commitment to address the broader issues of FRT reform. HTI has undertaken extensive work in this area, and has outlined a model law for FRT, which has achieved widespread multi-sector support.[8] This model law should be the foundation of broader reform in this area.

While the need is urgent and important, Parliament has a number of viable options regarding where to locate this broader FRT reform: it could be introduced into the Privacy Act, in a stand-alone FRT statute, in the IVS Bill or in another statute. Regardless of whether that broader FRT reform is included in the IVS Bill itself, the Committee is well placed to recommend that the Government introduce broader FRT reform as a matter of urgency. Until that broader reform takes place, Australians remain vulnerable to the significant harms associated with misuse and overuse of facial recognition. Moreover, schemes such as the IVS scheme also remain vulnerable to a catastrophic loss of community trust when the near-inevitable scandal occurs as a result of other organisations misusing FRT.

Recommendation 3: HTI recommends that the Government introduce legislation to regulate all forms of facial recognition technology, by implementing the Human Technology Institute's FRT model law.

[6] See, eg, Justin Hendry, 'Govt to ban one-to-many face matching by police', *InnovationAus.com* (News Article, 13 September 2023) <https://www.innovationaus.com/govt-to-ban-one-to-many-face-matching-by-police/>; Casey Tonkin, 'Govt plough ahead with facial recognition system', *ACS InformationAge* (News Article, 14 September 2023) <https://ia.acs.org.au/article/2023/govt-ploughs-ahead-with-facial-recognition-system.html>.
[7] Attorney-General's Department, *Government Response: Privacy Act Review Report* (Government Response, 28 September 2023) 10.
[8] UTS Human Technology Institute, *Facial recognition technology: Towards a model law* (Report, September 2022) <https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf>.

Redress for individuals & consequences for misuse

Under international law, Australia is obliged to ensure that there are effective and accessible remedies for individuals whose human rights are infringed. This includes people whose right to privacy is infringed.

HTI considers that the IVS Bill should be amended to improve the application of this important legal principle – especially by deterring more strongly entities that participate in the IVS scheme from breaching privacy provisions, and also by providing for more effective individual redress.

Consequences for misuse

As summarised below, the IVS Bill contains some provisions that seek to deter those who might misuse the IVS scheme. HTI considers these provisions are not strong enough given the inherent risks in the IVS scheme.

Clause 12 of the Bill provides for reporting of organisations' use of the IVS scheme, and an audit function. Where a party to a participation agreement does not comply with the terms of the agreement or an access policy, that party's access to the IVS scheme may be suspended or terminated. Similar provisions apply in cl 13 in relation to the NDLFRS hosting agreement.

Clause 21 makes it an offence (as outlined under section 136.1 of the *Criminal Code*) to make false or misleading statements in submitting a request for identity verification services. Clause 30 creates an offence that applies to 'entrusted persons' – that is, anyone (primarily public servants or a contractor acting on behalf of a government agency) operating the IVS scheme who have gained unauthorised access to, or made an unauthorised recording or disclosure of information obtained via the scheme. However, there are no explicit criminal offences, or civil penalties, within the IVS Bill for the misuse of protected information or the identity verification services by participating entities, including the Department.

Where misuse of identification information or the identity verification services by participating entities is a serious or repeated interference with the privacy of an individual, the civil penalty provisions under s 13G of the Privacy Act would apply – however, this civil penalty provision only applies to APP entities and therefore does not cover all participating entities in the IVS scheme. Additionally, where a participating APP entity experiences an eligible data breach (as defined under the Privacy Act), and the breach relates to information obtained or held due to its participation in the IVS scheme, the civil penalty provisions in s 13G may apply. However, a security breach under the IVS Bill will not necessarily invoke s 13G penalties, as the data breach must have been a serious or repeated interference with privacy related to an APP entity.

Given the IVS scheme involves large amounts of sensitive personal information, HTI considers that suspension or termination from using the identification verification services are not, on their own, sufficient to deter misuse of the IVS scheme. The IVS Bill should provide for more serious consequences for serious breaches – whether deliberate or through poor practices – to give stronger impetus for participating entities comply with their privacy and other obligations.

Recommendation 4: HTI recommends that the IVS Bill impose civil penalties or criminal offences in relation to the misuse of the identity verification services and identification information obtained through the identity verification services.

Redress for individuals

Where an individual suffers a breach of their right to privacy under the Privacy Act – or under a corresponding privacy law of a state, territory or New Zealand – the individual may seek to access the complaints and redress mechanisms that apply under the relevant privacy legislation. Thus, for example, a breach of Australia's federal Privacy Act would entitle an affected individual to make a complain to the Office of the Australian Information Commissioner (**OAIC**). The states, territories and New Zealand each have their own privacy regulatory body that performs similar functions to the OAIC.

If an entity accessing the IVS scheme breaches a provision of the participation agreement, this does not automatically entitle an individual affected by that breach to make a complaint to the OAIC or corresponding privacy regulator. This is because the individual is not a party to the participation agreement. Only if the entity's breach also amounts to a breach of the APPs (or equivalent state, territory or New Zealand privacy law provision) would the individual be able to make a complaint.

Individuals may also have limited recourse through the operation of the participation agreement or NDLFRS hosting agreement. Clauses 9(2)(d) (in relation to participation agreements) and 13(3)(d) (in relation to the NDLFRS hosting agreement) require that the relevant agreement must have arrangements in place for dealing with complaints by individuals whose identification information is held by the party in relation to the IVS scheme, which is reflected in cl 29 of the current FMS Participation Agreement and cl 13.8 of the NDLFRS hosting agreement. These provisions do not outline what remedies an individual may receive in relation to a complaint, just that the parties must have complaint mechanisms in place.

In any case, where an individual can access a privacy complaint mechanism, such as via the OAIC, there are significant practical barriers to achieving redress. The complaints mechanisms for most of Australia's privacy and information regulators have large backlogs of complaints, with insufficient resourcing to manage the complaints in a way that delivers swift redress.

Further, there is disparity across the States and Territories on the operation, rights and funding of their privacy and information commissions, meaning that individuals in different jurisdictions could be given different outcomes to other individuals who have been affected in an identical manner.

Individuals whose human rights and privacy have been affected by the actions of a participating entity in the identity verification services should have an effective process through which to submit a complaint about the entity's actions and be provided with redress proportionate to the harm they have suffered.

Recommendation 5: HTI recommends that 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. Such 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.

System-wide oversight of the IVS scheme

The IVS Bill vests oversight powers in the Information Commissioner – those powers apply to the IVS scheme as a whole, not solely in respect of individual complaints. In particular, cl 40 of the IVS Bill provides for an annual assessment of the operation and management of the approved identity verification facilities by the Information Commissioner and the production of a written report on the assessment.

Such systemic oversight, which goes beyond reliance on individual complaints, is vital to the effective, lawful and safe operation of the IVS scheme. However, HTI observes that these powers under the IVS Bill are less extensive than those usually provided to the Information Commissioner under other comparable legislative schemes. HTI considers that this deficiency should be addressed via amendments to the IVS Bill.

For example, the Information Commissioner, under s 33C of the Privacy Act, has various powers to conduct, "in such manner as the Commissioner considers fit", assessments to ensure compliance with the APPs.[9] Section 33C provides a general power for the Information Commissioner to conduct assessments in relation to APP entities and their compliance with the APPs and additional powers in relation to some government schemes that require additional privacy oversight, such as the handling and matching of information under the *National Health Act 1953* (Cth). In relation to the IVS Bill, this gives the Information Commissioner power to conduct an assessment of the Department (as an APP entity) but does not provide them with broader oversight and assessments powers in relation to the IVS scheme as a whole or any non-APP entities that interact with the scheme (such as State or Territory government authorities, local government authorities or New Zealand entities).

The power under s 33C of the Privacy Act provides the Information Commissioner with considerable independence in conducting their assessments, which is necessary for accountability and effective delivery of services and gives credibility to the operation of not only the OAIC as an independent public body, but also to the government services that the Information Commissioner conducts assessments for. Additionally, HTI notes that the Digital ID Bill proposes to amend s 33C of the Privacy Act (with a new s 33C(1)(g)) to explicitly give assessment powers to the Information Commissioner in relation to the handling and maintenance of personal

[9] *Privacy Act 1988* (Cth) s 33C(2).

information under the Digital ID Bill.[10] Due to the sensitive nature of the information handled under the IVS scheme, greater oversight of the IVS scheme's privacy procedures and practices is required, which HTI believes could be provided through amendment to s 33C to give the Information Commissioner specific powers to assess the IVS scheme's operation, similar to the proposed powers to be given in relation to the Digital ID Bill.

Further, under cl 40 of the Digital ID Bill, the Information Commissioner, in addition to the powers in s 33C of the Privacy Act, is granted the function of providing advice on the operation of the Digital ID Bill to the Digital ID Regulator on the regulator's request. This inclusion indicates a recognition of the upmost importance of privacy under the digital ID system and acknowledgement of the ongoing need for review and ad hoc changes to services that handle sensitive information. HTI considers that a similar power should be granted to the Information Commissioner under the Bill to ensure ongoing review and uplift of the privacy mechanisms in the identity verification services and involvement of the Information Commissioner in matters related to privacy.

The Explanatory Memorandum to the IVS Bill does not explain why the Information Commissioner has less extensive powers under the IVS scheme. HTI considers that giving the Information Commissioner more limited powers undermines their ability to conduct their systemic oversight function and could result in a larger number of system-wide problems throughout the identity verification process that are more difficult to resolve.

HTI proposes that the powers granted to the Information Commissioner under other legislation could guide the amendments that should be implemented in the IVS Bill to ensure the Information Commissioner is given sufficient independence and powers to effectively conduct their assessments.

Recommendation 6: HTI recommends that the IVS Bill and Privacy Act be amended to provide the Information Commissioner with greater powers and independence in relation to their assessment function, including by:

(a) inserting a new provision in s 33C of the Privacy Act to allow the Information Commissioner to conduct an assessment of the operation and management of the IVS scheme and IVS Bill, which may be conducted in such manner as the Information Commissioner sees fit

(b) inserting a provision similar to cl 40 of the Digital ID Bill 2023 to provide the Information Commissioner with an advisory role in relation to the operation of the Bill at the request of the Minister.

Other drafting issues

HTI considers that some of the drafting of the IVS Bill is ambiguous and could be improved with a view to aiding the interpretation of the IVS Bill. By way of example, in practice, the operation of the DVS and FVS systems, and process through which requesting entities request these services, are very similar;

[10] Digital ID Bill 2023 (Cth) cl 44(4)(d).

however, the descriptions of the request-to-response process outlined in relation to each of the services (cls 15 and 19-20 respectively) are vastly different. These descriptions could be more closely aligned to describe more clearly the steps to be undertaken to access the DVS and FVS and assist in interpreting the IVS Bill as a whole.

Further, there is inconsistency in the terminology used throughout the IVS Bill, which creates confusion regarding the operation of the IVS scheme and what requesting parties may receive in response to a request for identity verification services. For example, in the definitions of DVS, FVS and FIS, there is inconsistent use of the terms 'response' and 'outcome'. In relation to a DVS or FVS request, the requesting party receives a 'response' (cls 15(1)(h) and 19(e) respectively), whereas an FIS request produces in an 'outcome' (cl 16(d)). Neither 'response' nor 'outcome' is defined in the IVS Bill.

The natural and ordinary meaning of 'response' appears to encompass a broader range of potential results that may be provided to a request (eg, a 'match' or 'no match' response, or the provision of identification information) than 'outcome', which suggests a more definite, clear-cut result (eg, only a 'match' or 'no match' response). However, these interpretations do not align with the actual results that may be provided for each identity verification service, particularly as a DVS result can only ever be 'match' or 'no match', while FVS and FIS can provide both 'match' or 'no match' results, and provision of facial images and other face-matching service information.

Recommendation 7: HTI recommends that the drafting of the IVS Bill as a whole be reviewed and amended to more clearly and effectively describe the IVS scheme, its operation and the rights and responsibilities of individuals and participating entities to ensure easier interpretation of the IVS Bill.

Training for facial recognition and image comparison

Under cls 10(2)(b) and 17 of the IVS Bill, relevant staff requesting FVSs or FISs, where a facial image may be provided in a response or handling facial images provided in a response to an FVS or FIS request, must be "trained in facial recognition and image comparison". Only parties that are government authorities are to be provided with facial images as a response to an FVS or FIS request, with only certain law enforcement agencies permitted to access FISs.

"Facial recognition and image comparison", and the training required in relation to this, are not defined in the Bill, which makes it unclear what each person must do in order to comply with this requirement. Paragraph 189 of the Explanatory Memorandum states that "it is proposed that the participation agreement will provide further detail about training requirements and standards". Clause 24.3 of the current FMS Participation Agreement, which outlines the current training requirements and standards, provides that the "relevant training package" will be supplied by the Hub Controller. However, this provision in the Agreement does not specify what this training package includes and what knowledge persons receiving facial images must have before being considered to have sufficient "facial recognition and image comparison" training.

Additionally, the FMS Participation Agreement allows for alternative training arrangements to provide persons with a similar or greater level of knowledge than is provided under the relevant training package.[11] Allowing alternative training arrangements has the potential to create discrepancies between the abilities of persons permitted to receive facial images, which could result in facial images not being protected to the standard required in certain circumstances.

While the Bill imposes training requirements on government authorities requesting facial images through the FVS or FIS, it does not impose similar obligations on the Department and persons tasked with handling and providing facial images to other government agencies. HTI considers that where a training obligation is placed on one party for the purpose of avoiding misuse of the identity verification services and any facial images received in response to a request, an identical obligation should be placed on the Department to ensure that *all* persons handling facial images (whether on behalf of the Department or as a receiving party) are held to the same training and standard requirements. Individuals whose facial images are handled in relation to the identity verification services expect and should receive the same protection of those images, no matter where in the request-to-response pipeline they are handled.

Recommendation 8: HTI recommends that:

(a) "facial recognition and image comparison", and the training requirements in relation to this activity, be specified in the relevant participation agreements or access policies for FVS and FIS

(b) all Department officers, members of staff, employees, contractors and employees of contractors who handle facial images in relation to a request for FVS or FIS be required to undertake the same facial recognition and image comparison training that persons receiving images undertake.

Statutory review of the IVS scheme's operation

Clause 43 of the IVS Bill requires the Minister to review the operation of the Bill and the provision of identity verification services within two years of the commencement of the IVS Bill.

We note that the Government has indicated that passage of this Bill is urgent, and that there is very limited capacity for meaningful public consultation. Moreover, the Bill is being introduced in an area where the stakes are high for individuals, and the scheme itself is very large. As noted above, in a recent 12-month period, the DVS was used over 140 million times, and there were approximately 2.6 million FVS transactions.

Perhaps most critically of all, the IVS Bill is intimately connected to two other major reform processes. Firstly, the IVS Bill does not align in key respects with

[11] Face Matching Services Participation Agreement cls 24.3(b)(ii) and 24.3(c)(ii) <https://www.idmatch.gov.au/Documents/FMS%20Participation%20Agreement%20-%20conformed%20copy%20-%20_Redacted.pdf>.

the Digital ID Bill. This misalignment is a major deficiency: it leads to inferior privacy protections for Australians, and it increases the cost of compliance for government and business as there are two inconsistent schemes operating in an overlapping area of activity.

Secondly, the primary protections for individuals in the IVS Bill are set out in the Privacy Act, which the Government acknowledges needs to be amended as soon as possible. Prior to the Privacy Act being amended, Australians will be subject to inferior privacy protections under the IVS Bill.

For these reasons, and given the need for a more extensive set of transitional arrangements than would normally be the case for a Bill of this nature, we recommend that the IVS Bill be amended to provide for an interim review after one year. That one-year review should focus on the adequacy of the privacy protections – under the IVS Bill, any rules made pursuant to cl 44, and / or the Privacy Act (as applicable).

Recommendation 9: HTI recommends that cl 43 of the IVS Bill be amended to provide for an interim review of the operation of this law after 12 months. That interim review should focus on the adequacy of the privacy protections operating in the IVS scheme.