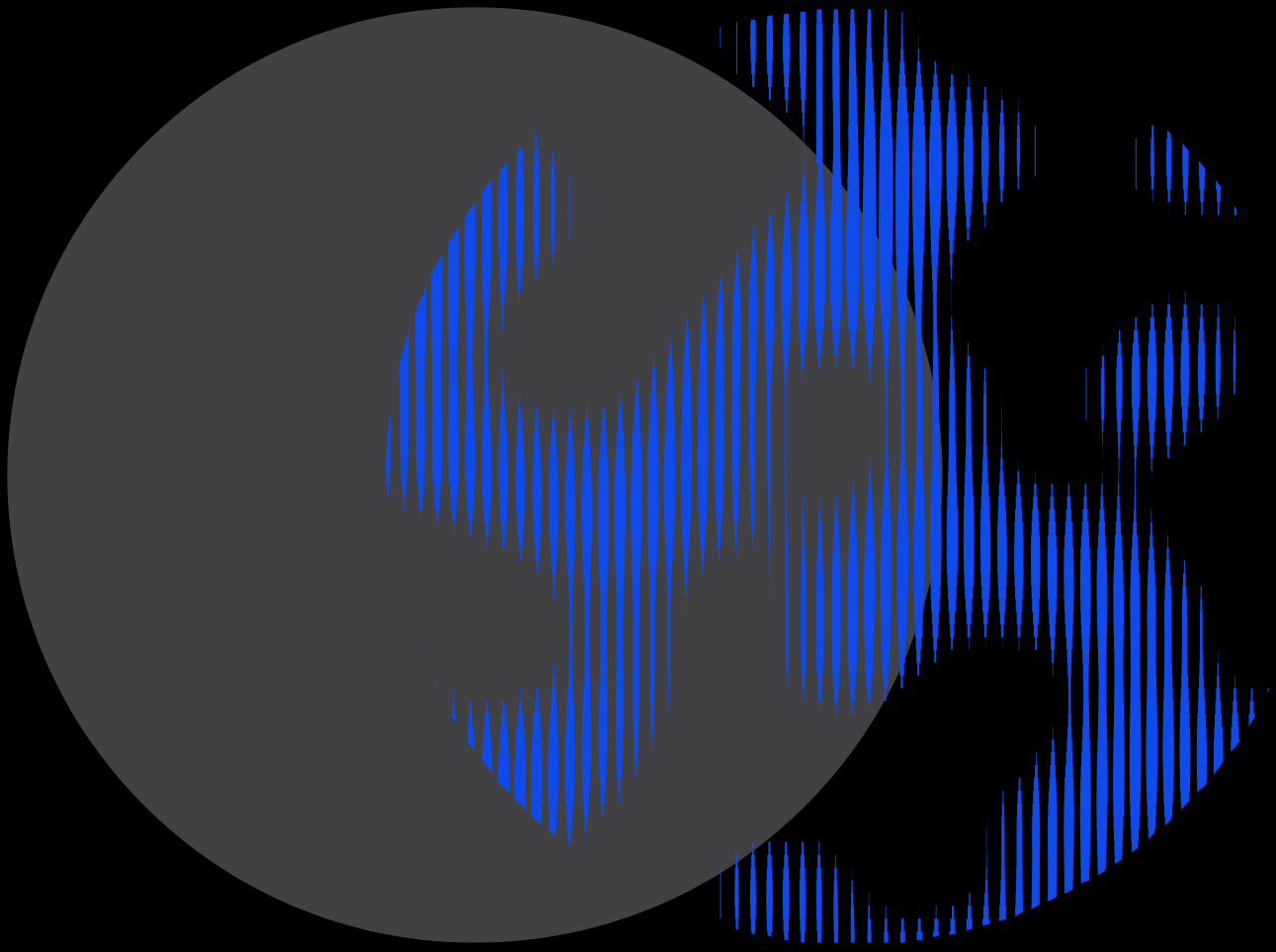
Human Technology Institute



Consultation on Identity Verification Services Rules

26 April 2024

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.

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: Sarah Sacher and Professor Edward Santow

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

Submission on Draft Identity Verification Services Rules

The Human Technology Institute (**HTI**) welcomes the opportunity to make a short submission to the Attorney-General's Department on the Draft Identify Verification Services Rules (**Draft Rules**).

HTI notes that the Draft Rules, as currently proposed, deal primarily with the levying of fees. We do not have any advice on these provisions.

We observe that the Attorney-General has a broad power to make subordinate legislation: s 44(1) of the *Identity Verification Services Act 2023* (Cth) (**IVS Act**) states that the Attorney-General 'may make rules prescribing matters required or permitted by the Act to be prescribed in the rules, or necessary or convenient to be prescribed for carrying out or giving effect to the Act'. This would enable the Attorney-General to address some of the concerns raised by HTI and other stakeholders during consideration of the Identity Verification Services Bill 2023 (as it then was) – a number of these concerns were raised also by the Senate Legal and Constitutional Affairs Legislation Committee. In saying this, we acknowledge that there are real limits in how far subordinate legislation can go in addressing issues with primary legislation.[1]

More specifically, we consider there to be scope within the general rule-making power conferred by s 44(1) to address known issues with the IVS scheme and improve its administration, including to improve consistency across the digital ID scheme as a whole; and to practically realise principles of transparency, redress and fair decision making.

In September 2023, HTI made a submission on the IVS Bill to the Senate Legal and Constitutional Affairs Legislation Committee, outlining key concerns with the Bill as it stood at the time.[2] HTI noted that the IVS Act is only one part of the Australian Government's broader digital identity scheme, with the other parts of this scheme to be governed primarily by the Digital ID Bill 2024. The digital identity scheme also relies on privacy protections in the *Privacy Act 1988* (Cth) (**Privacy Act**), which is overdue for reform. The fact that the IVS Act, the Digital ID Bill 2024 and the Privacy Act are not fully harmonised in terms of their privacy obligations, redress mechanisms and oversight provisions creates regulatory uncertainty, which reduces the privacy protections for individuals and adds to the compliance burden for relevant government and private sector participants in the digital identity scheme.

We welcome the fact that, prior to the passage of the IVS Act, key amendments were made that brought it into better alignment with the stronger privacy protections in the Digital ID Bill. However, there are ongoing issues associated with the digital identity regime being governed by three different legislative instruments. These should be addressed.

We recommend close coordination with the Department of Finance, the Digital ID Regulator and the Office of the Australian Information Commissioner to ensure that these laws are administered in a consistent and coherent manner. HTI recommends that the Draft Rules be extended to address the following areas of overlap and uncertainty:

[1] See, especially, *South Australia v Tanner* (1989) 166 CLR 161.
[2] Human Technology Institute submission to the Legal and Constitutional Affairs Committee, *Inquiry into the Identity Verification Services Bill* (September 2023).

- **Privacy protections**. The Attorney-General's Department should analyse the Digital ID Bill and the IVS Act for inconsistencies relating to privacy protections, and develop rules designed to minimise these inconsistencies, in alignment with future rules to be administered under the Digital ID Bill. While we have not been in a position to undertake a comprehensive analysis of these inconsistencies, one example is provisions around data retention. Although both the IVS Act and Digital ID Bill provide for destruction of data, the relevant provisions are not fully aligned – the Digital ID Bill has more specific provisions regarding the 'immediate' destruction of biometric data (cl 51), along with destruction of other personal data (cl 136). The IVS Act requires parties to participation agreements to take 'reasonable steps to destroy each facial image of an individual, as soon as is reasonably practicable' (s 10(2)). Neither instrument provides a clear data retention period – there is scope for clarification and alignment across both Digital ID Rules and IVS Rules, on practical expectations around data retention and destruction.

- **Redress**. The IVS Scheme specifically, and the broader digital identity scheme, should provide for a single body to provide oversight, complaint handling and redress. This would make individual and systemic problems easier to identify and resolve—both for individuals, as well as for government and private sector bodies engaging with these schemes. However, the IVS Act does not provide for a single body to perform these functions.

- **Law enforcement reporting.** HTI has previously expressed concern about the extent to which law enforcement (and intelligence services) are able to access personal data across the digital identity scheme. To improve community trust and accountability over this access, the Rules should provide for greater transparency with respect to the IVS scheme, by explicitly adopting the requirements contained in the Digital ID Bill for law enforcement reporting. This includes requirements for law enforcement to report on the number of information requests, the types of information requested, and the total number of requests, and outline this in an annual report made by the AFP Minister (cl 155A and 155B).

In addition to the above, we suggest that provision be made in the Rules for training requirements. Section 10(2)(b) of the IVS Act provides that 'a participation agreement must provide for each party to the agreement that proposes to request identity verification services' to be 'trained in facial recognition and image comparison'. However, the nature of this training is not prescribed. Additionally, while the Act imposes training requirements on government authorities requesting facial images, it does not impose similar obligations on the Department and persons tasked with handling and providing facial images to other government agencies.

Facial recognition and image comparison involves the handling of highly-sensitive information, and there are known risks of misidentification and algorithmic bias associated with facial recognition technology. The Rules should therefore outline the specific kinds of training required, to ensure that training is conducted to a high quality. The Rules should also require everyone involved in the handling of facial images to undertake the same training.