Human Technology Institute

Submission to the Privacy Act Review Report consultation

March 2023

March 2023

Authors: Sophie Farthing, Lauren Perry, Professor Edward Santow

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

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

Executive Summary

The Human Technology Institute (**HTI**) strongly supports the case for privacy reform outlined in the *Privacy Act Review Report 2022* (**the Review Report**).

Australia's privacy law is no longer fit for purpose. New and emerging data-driven technologies, particularly artificial intelligence (AI), collect, process and store personal information in unprecedented ways.

There is increasing community concern regarding how personal information is being used, along with a growing expectation that the Government will strengthen regulation to ensure that Australians, and our economy, benefit from positive technological innovations while being protected from harm.

Amid the rise of new and emerging technologies such as AI, there is an important and urgent need to reform the Privacy Act. The Government should act now.

In this submission, HTI broadly supports the Review Report's combination of proposals that, if implemented, will empower individuals to manage the use of their personal information in certain circumstances, and impose additional obligations on entities to actively protect and manage risks associated with their use of personal information.

This submission focuses especially on the need to reform Australian law relating to facial recognition and other biometric technologies. In particular, the development and use of facial recognition technology (FRT) in Australia is largely unregulated. Current law does not adequately address the risks of harm associated with FRT, nor does it encourage or incentivise positive innovation with FRT.

We call on the Government to implement the recommendations from HTI's report, *Facial recognition technology: Towards a model law* (**the HTI FRT Model Law**), published in September 2022. HTI welcomes the positive reference to the HTI FRT Model Law in the Review Report, and urges the Government to amend Australia's privacy law so it sets an appropriate balance that addresses the risks of harm associated with FRT, while encouraging positive innovation with FRT.

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.

To inform its submission, HTI draws on several of its major projects:

Facial Recognition Technology: Towards a Model Law

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

The Future of AI Regulation in Australia, that will consider the major legal and policy issues related to AI and present a roadmap for reform

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

Introduction

On 23 February 2023, the Attorney-General released his Department's *Privacy Act Review Report 2022* (the Review Report). The Attorney-General has provided a further opportunity for consultation on the Review Report, prior to the Government finalising its response to the Review Report and, more specifically, the Government's position on reform of Australian privacy law. The Human Technology Institute (HTI) welcomes the opportunity to make a submission to this process.

HTI is an independent non-profit organisation, which is part of the University of Technology Sydney (UTS). HTI applies human values to new technology. HTI works with communities and organisations to develop skills, tools and policy to ensure new and emerging technologies are fair and inclusive.

Australia's privacy law was drafted largely before the internet, and well before the rise of new and emerging technologies such as artificial intelligence (AI). This technological transformation has been described as the Fourth Industrial Revolution, a description that conveys the enormity of change happening to our economy and society. Much of this new technology relies on data, and especially our personal data, and so there are especially profound implications for our right to privacy, along with a range of other human rights such as the right to non-discrimination.

Powerful new technologies, such as AI and automated decision making, are already ushering in major change: some of this change benefits individuals and society, and some causes significant harm. There is an urgent need to modernise Australian law, and especially privacy law, to improve our ability to harness the opportunities for benefit, while guarding more effectively against the threats.

HTI commends the extensive consultation supporting the proposals in the Review Report. In addition to this Review's two previous rounds of public consultation, the Attorney-General's Department has had the benefit of several major Australian Government privacy reform processes, which involved their own significant public consultations, including two privacy reviews by the Australian Law Reform Commission since 2005.

It must also be acknowledged that many of the recommendations from previous privacy reform processes remain unaddressed. This adds to the urgency of the need for reform. Australia has reached a pivotal moment: Australia must modernise its privacy protection framework to better address the challenges posed by new and emerging technologies that are deployed to collect, store and use personal information. HTI urges immediate action by the Government to reform Australia's Privacy Act, and better equip Australians for the future.

The impact of technology on privacy: the need for reform

New and emerging technologies engage a range of human rights. The impact on people can be positive and negative, often affecting particular groups within our community differently. The scale and speed of this technological impact is almost certainly unprecedented in human history. Regulation for this new era must be technologically well informed, responding to and where possible anticipating issues related to new technology. The goal should always be to ensure that humans experience the benefits of new technology, while addressing or at least mitigating the risks.

Privacy regulation is a fundamental feature of the regulatory framework and is needed to address the risks posed by new and emerging technologies.

Privacy is a multifaceted human right, enshrined in international law by Article 17 of the *International Covenant on Civil and Political Rights (*ICCPR), to which Australia is a party. The right to privacy underpins many other fundamental rights – such as freedom from discrimination and freedom of association, religion, thought and expression – because it provides an important brake against the misuse and overuse of individuals' personal data. While the right to privacy is not an absolute right, this right cannot be limited or restricted arbitrarily. International law sets the default position that an individual's right to privacy must be respected. The right to privacy

may be limited only in certain circumstances, set out in international law itself, with any limitation on the right to privacy subject to the *Siracusa Principles*.

Australian privacy law focuses on protecting personal information. Personal information is the fuel for data-driven technologies, such as AI, that have proliferated in recent years.

Personal information is collected and used in the training, development and operation of AI systems. Often, personal information is shared and amalgamated from multiple sources. Generative AI, for example, is trained on vast amounts of publicly available data, including personal information. Outcomes of these systems can have a significant impact on the individual, but also carry broader societal risks.

The way information is used in AI systems makes for a complex operating environment. It is necessary for that complexity to be addressed thoughtfully and effectively by a range of regulatory measures directed towards addressing the risk of harm and encouraging safe, positive innovation.

Australians are becoming increasingly aware of the risks associated with the widespread collection and use of personal information and expect government to provide higher levels of protection than are currently available.[1] Research into the social perception of AI regulation has shown that Australians expect AI to be regulated by government (alongside regulators and independent AI bodies), over self-regulation by industry, and that the current regulatory regime is insufficient to ensure the safety of AI use.[2]

Comparable jurisdictions all over the world are grappling with the regulatory challenges posed by new and emerging technologies, and particularly new generations of AI. It is widely recognised across almost all stakeholder groups that Australia's current privacy law is not fit for purpose and is in urgent need of reform. Against a broader consideration of the implications of AI and automation, HTI supports the proposals made in the Review Report (as outlined in the table below) and urges the Government to legislate to address these ongoing risks.

Facial recognition technology

HTI welcomes proposals in section 13 of the Review Report to mandate risk assessments for activities posing a high risk to privacy. HTI particularly endorses the Report's conclusion that biometric technologies pose a high risk to privacy, and the Review Report's commitment to consider the HTI FRT Model Law.[3]

A risk-based approach

As a general principle, HTI supports the Review Report proposals to require regulated entities considering an activity that poses a high risk to privacy to undertake a risk assessment. This approach can facilitate innovation, while also protecting human rights.

There is precedent for an enhanced risk impact assessment regime from overseas jurisdictions. Research on the effectiveness of data protection impact assessments (DPIAs) required under the EU's General Data Protection Regulation (GDPR), for example, suggests DPIAs can be a useful tool to identify potential risks, understand how those risks may be viewed by the general public, and set out the steps needed to mitigate those risks prior to implementation.[4]

The HTI FRT Model Law, published as an outline in September 2022, adopts a regulatory approach that relies on a form of DPIA and is entirely consistent with the approach taken in the

[1] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2020* (Report, September 2020) 65–66.
[2] Nicole Gillespie et al, *Trust in Artificial Intelligence: a global study* (Report, 2023) 37–38.
[3] Australian Government, Attorney-General's Department, *Privacy Act Review Report* (Report, 2022, published 16 February 2023),126.
[4] Felix Bieker et. al., 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation' (Conference Paper, Annual Privacy Forum, 7–8 September 2016); Gizem Gültekin Várkonyi and Anton Gradišek, 'Data Protection Impact Assessment Case Study for a Research Project Using Artificial Intelligence on Patient Data' (2020) 44(4) *Informatica*; Michael Friedewald et al, 'Data Protection Impact Assessments in Practice: Experiences in Case Studies' (Conference Paper, Workshop on Security, Privacy, Organizations, and Systems Engineering, European Symposium on Research in Computer Security, 7–8 October 2021).

Review Report itself. More specifically, the HTI FRT Model Law proposes the creation of a Facial Recognition Impact Assessment (FRIA) process for all activities engaging the use of facial verification, identification or analysis. The FRIA model was developed following extensive consultation with a range of industry leaders, government representatives, academic experts and civil society organisations, as well as drawing on qualitative research and other recent official public consultation processes.[5]

A FRIA would involve the rigorous consideration of specific matters in the process of development and deployment of FRT applications. The HTI FRT Model Law would prohibit FRT applications that have been assessed as high risk in the FRIA process, except in some limited contexts. Exceptions to this general prohibition include:

- where the regulator considers that the use of a high-risk FRT application is justified under international human rights law. An example of this could be where a facial analysis tool is used by people who are blind or vision impaired to 'read' the emotions of people around them
- specific law enforcement and national security reasons, and subject to additional protections
- genuine academic research following appropriate legal and ethical protections.

A key advantage of the risk-based FRIA approach is that it would allow Australians, including government and business, to enjoy the benefits of lower-risk uses of FRT (such as facial verification for accessing personal accounts online), while protecting citizens from the increasing number of potentially harmful uses of the technology (such as employers rolling out facial identification or analysis for behavioural surveillance in workplaces).

Immediate reform to regulate FRT

The Privacy Act already recognises that biometric information is a sensitive form of personal information that requires additional protections. The advent of new technologies that process biometric data, such as FRT, pose a new and significant risk to privacy, which must be addressed.

FRT implicates an especially sensitive subset of personal information – namely, biometric information. Faces contain unique information about individuals, including information relating to protected attributes such as sex, age, race and disability status. Because faces are 'public', they can be captured or surveilled without an individual's awareness, let alone consent. The use of biometric data in FRT systems can enable deployers of these technologies to infer, or try to infer, highly personal information about individuals, which can be used to make legal and similarly significant decisions about those individuals.

It is generally recognised that current Australian law does not adequately regulate the development and deployment of FRT. Given increasing evidence of the harms caused by the unregulated use of FRT, both in Australia and abroad (see Table 1 below), this must urgently change.

The FRIA model proposed by HTI is based on extensive feedback and endorsement, forming a strong case for change. HTI accordingly urges the Attorney-General to lead a national process of legislative reform in this area. This could be via timely amendments to the Privacy Act itself, or through a standalone piece of legislation that operates by reference to the general schema of the Privacy Act.

Table 1 – Recent examples of unregulated use of FRT

Date	Use of FRT
December 2021	The OAIC determined that the Australian Federal Police failed to comply with its privacy obligations through its use of a Clearview AI FRT tool.[6]

[5] Human Technology Institute (UTS), *Facial recognition technology: Towards a model law* (Report, September 2022), 22-24; 84-86.
[6] Office of the Australian Information Commissioner, Government of Australia, 'AFP Ordered to Strengthen Privacy Governance', News and Media (Web Page, 16 December 2021) https://www.oaic.gov.au/updates/news-and-media/afp-ordered-to-strengthen-privacy-governance.

June 2022	A CHOICE investigation revealed the covert use of FRT by Bunnings, Kmart and the Good Guys for security and theft prevention.[7]
December 2022	Entertainment venues in New York, USA, Madison Square Garden and Radio City Music Hall, deployed FRT to ban the entry of lawyers working for firms engaged in legal action against the company running the venues.[8]
January 2023	Football Australia revealed that FRT had been used to identity and expel six blacklisted fans from an A-League football grand final in Sydney in 2017.[9]
February 2023	The US Air Force completed a project for the deployment of reconnaissance and surveillance drones outfitted with FRT capabilities for special operations.[10]

[7] Jarni Blakkarly, 'Kmart, Bunnings and The Good Guys Using Facial Recognition Technology in Stores', CHOICE (Web Page, 2 August 2022) <https://www.choice. com.au/consumers-and-data/data-collection-and-use/how-your-data-is-sed/articles/kmart-bunnings-and-the-good-guys-using-facial-recognitiontechnology-in-store>.
[8] Kashmir Hill and Corey Kilgannon, 'Madison Square Garden Uses Facial Recognition to Ban its Owner's Enemies', *New York Times* (online, published 22 December 2022, updated 3 January 2023) https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html.
[9] Vince Rugari, 'A dystopian future? Why facial recognition may be coming to a stadium near you', *The Sydney Morning Herald* (online, 12 January 2023) https://www.smh.com.au/sport/soccer/a-dystopian-future-why-facial-recognition-may-be-coming-to-a-stadium-near-you-20230111-p5cbrd.html.
[10] David Hambling, 'US Air Force is giving military drones the ability to recognise faces', *New Scientist* (online, 23 February 2023) https://www.newscientist.com/article/2360475-us-air-force-is-giving-military-drones-the-ability-to-recognise-faces/.

HTI responses to key proposals in the Review Report

Proposal	HTI Position	Additional comment
Proposals 3.1, 3.2 Amend the objects of the Act	Support	No additional comment.
Proposals 4.1-4.8 Definition of 'personal information'	Support	HTI supports the proposals to clarify, and expand, the definition of 'personal information'. The proposed amendments to the Privacy Act will address the ways that new technologies, such as AI, have changed how 'personal information' is collected, processed and used, including through drawing inferences from amalgamated data sets collected from individuals, where consent may not ever have been given. To address the impact of how information is processed by AI, HTI recommends that 'reasonably identifiable' be understood to include where an individual is distinguished from others in a group, even if their identity is unknown. HTI also supports the creation of industry codes and regulator guidance, to support the Act's adaptation to new technologies. As a general principle, HTI recommends any guidance or lists of examples intended to guide APP entities be contained in OAIC guidance, rather than solely in explanatory materials for legislation.
Proposal 4.9 Amending the definition of sensitive information	Support	HTI supports amending the definition of 'sensitive information', particularly given the way that certain AI (especially machine learning) tools process information by categorisation and inference. HTI notes that APP entities would be assisted by the development of guidance that contains a non-exhaustive list of examples of where sensitive information may be inferred from non-sensitive information.
Proposals 6.1 to 9.5 Exemptions to the Privacy Act	Support	HTI supports the removal of the small business exemption in proposal 6.1. There is no reason, in principle, to exempt a company on the basis of its size from the requirement to respect the human right to privacy of individuals it affects. The growth and democratisation of new technologies like AI mean that even small organisations may have a significant, scalable impact on individuals. At least while the Government conducts further consultation on these Proposals, HTI strongly supports an immediate amendment of the Privacy Act to ensure the small business exemption does not apply to the use of FRT (proposal 6.2). As outlined above, FRT poses a particular risk given the sensitivity of the personal information collected, and the significance of potential harm that stems from the use of biometric information. Generally, regarding the exemptions contained in the Privacy Act, HTI notes that limitations on the right to privacy can be justified only by reference to the strict requirements in international human rights law. Hence, it

		is difficult, if not impossible, to justify any exemption from the requirements of privacy law that applies to an entire category of legal person (such as in respect of journalism and political parties). All such blanket exemptions should be replaced by more targeted limitations on the right to privacy, which conform with international human rights law.
Proposals 10.1 to 10.3; 11.1 to 11.4 Privacy and collection notices Consent and online privacy settings	Support	HTI supports amending the Act to ensure privacy and collection notices are clear, current, understandable and accessible. HTI agrees with the Review Report that these two types of notices should remain distinct in order to remain clear and concise, and therefore more easily understood by individuals. HTI also considers requiring an entity to deliberately consider and communicate the implications for an individual's personal information in a privacy notice will increase awareness and transparency around data collection. HTI also supports amendment to facilitate informed consent, noting that the concept of informed consent alone is insufficient to address the risks associated with the use of personal information by technological applications such as AI.
Proposals 12.1, 12.2, 12.3 A fair and reasonable test for the collection, use and disclosure of personal information	Support	HTI supports the inclusion of a fair and reasonable test to govern the collection and use of personal information. As an overarching principle, HTI agrees it is vital that individuals do not continue to bear the burden of ensuring their personal information is not used against them; the fair and reasonable test will go some way to shifting that burden. HTI also welcomes the development of guidance to support the assessment of whether the collection and use of personal information is fair and reasonable in the circumstances, but recommends this be included —as a non-exhaustive or indicative list— in the Act itself, or developed in OAIC guidance, rather than solely in the explanatory material supporting a Bill.
Proposals 13.1, 13.3, 13.4 PIAs for high privacy risk activities	Support	HTI supports the mandatory completion of a PIA for all activities that carry a high privacy risk. To support transparency regarding high-risk activities, HTI recommends PIAs be made publicly available on an OAIC online database (rather than requiring PIAs to be made available to the public only following an OAIC request for it). HTI supports the development of OAIC guidance regarding what activities will be considered to carry a high privacy risk. In the HTI FRT Model Law, HTI sets out a non-exhaustive list of factors relevant to assessing the risks associated with an FRT application, such as the special context of use and deployment, the functionality of the application, and the FRT application's role in decision making, including whether the decision being made is partially or wholly automated.[11]

[11] Human Technology Institute (UTS), *Facial recognition technology: Towards a model law* (Report, September 2022), Part 7.

		To support effective regulation, HTI also supports the development of practice-specific guidance where new and emerging technologies poses a risk to privacy. The HTI FRT Model Law stresses the regulator's important role in providing clear, accessible and expert advice on privacy law and associated practices to both organisations and affected individuals.[12] To fulfil this function effectively, the regulator needs to be appropriately resourced and upskilled.
Proposal 18 Individual rights related to personal data	Support	HTI supports giving individuals greater rights in relation to how their personal data is used. De-indexing internet search results (Proposal 18.5), for example, will give individuals some control over how their personal information is used. This is particularly important given emerging technologies, such as generative AI, rely on massive amounts of publicly available information to train the system and develop outputs, posing a greater risk that an individual's personal information may be used without their knowledge, including for malicious purposes. HTI also supports the introduction of the right to erasure of personal information (Proposal 18.3), but seeks further detail regarding when and how information will be quarantined. Where there is any retention of personal information to enable third party access, it is important that there are clear guardrails in law to protect privacy. While some of this may appear in regulation and guidelines, access by third parties, as a general principle, should be contained in primary legislation.
Proposal 19 Automated decision-making	Support	HTI supports the section 19 proposals that will require APP entities to disclose how personal information will be used in automated or substantially automated decisions which have a legal, or similarly significant effect on an individual's rights. This is an important step to support transparency and accountability regarding the use of automated decision-making tools and systems. HTI recommends that it be made clear that 'substantially automated' includes situations where an inference, prediction or recommendation is produced by an automated system which may then be used by a human to make a final decision. HTI also recommends privacy policies indicate the types of substantially automated decisions that will be undertaken, in addition to the types of personal information that will be used. This will support Proposal 19.3, the right of individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made.

[12] Human Technology Institute (UTS), *Facial recognition technology: Towards a model law* (Report, September 2022), 81.