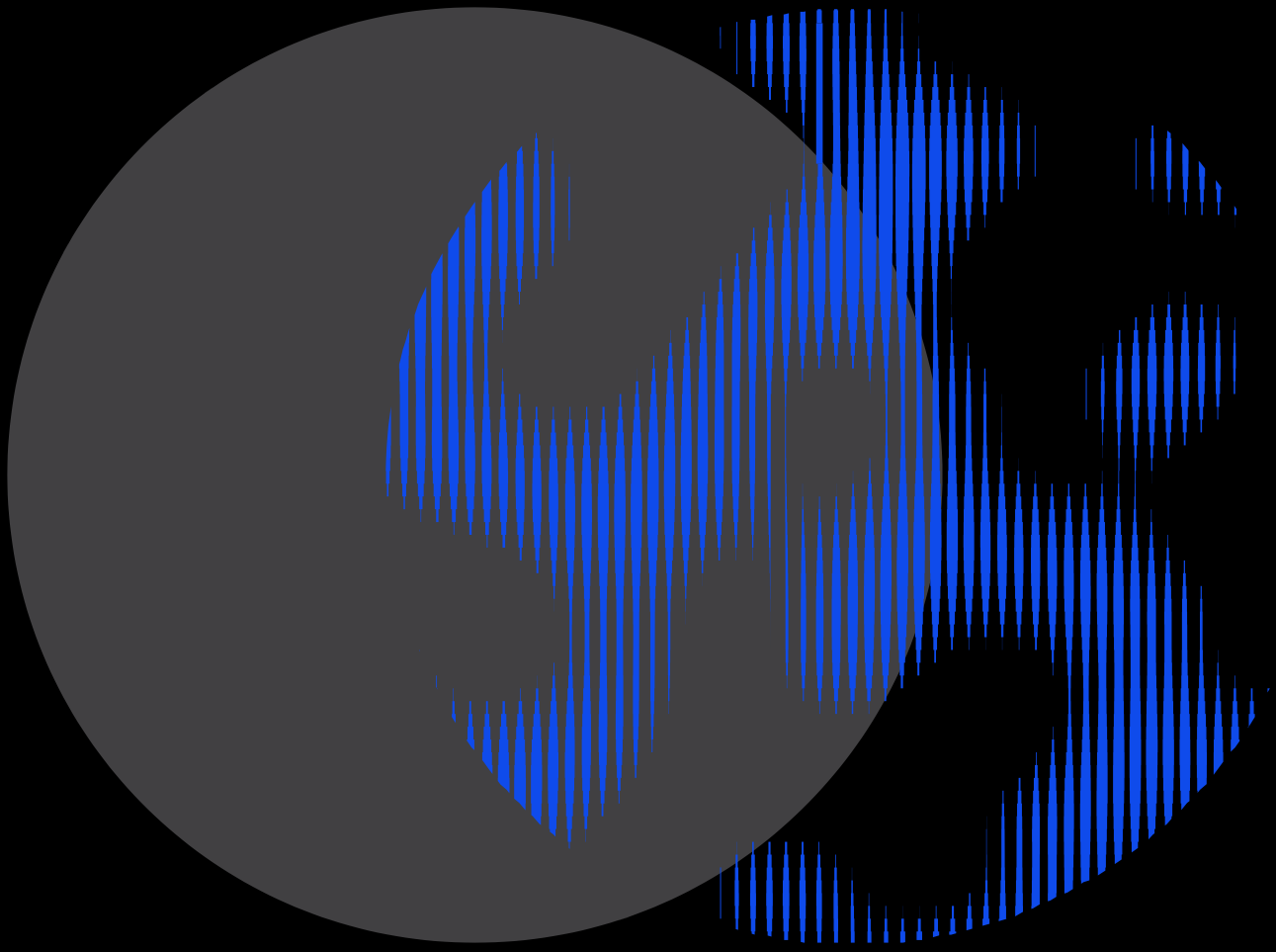
Human Technology Institute



Submission to the Legal and Constitutional Affairs Committee inquiry into the Privacy and Other Legislation Amendment Bill 2024

11 October 2024

11 October 2024

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

Authors: Sophie Farthing, Sarah Sacher and Prof Edward Santow

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.

11 October 2024

Contents

11 October 2024

Executive summary

The Human Technology Institute (HTI) welcomes the introduction of the Privacy and Other Legislation Amendment Bill 2024 (Cth) (the Bill) as the first step in strengthening the *Privacy Act 1988* (Cth) (the Privacy Act).

HTI particularly welcomes the Bill's creation of a statutory tort for a serious, unjustifiable infringement of the human right to privacy. This will provide protection for individuals from some of the worst forms of privacy breach, and provide for a right to a remedy for some people affected by such privacy violation. HTI also supports the Australian Privacy Commissioner developing a new Children's Online Privacy Code to protect children from a range of harms that kids experience simply by sharing their personal information.

This Bill should be seen as an important first step in reforming the Privacy Act. This reform is long overdue, and much more is needed to modernise Australia's privacy law for the 21st century. HTI urges the Government to act on the vast majority of its commitments to reform the Privacy Act, which are not reflected in this Bill, and which are necessary to address some of the most urgent and serious privacy threats facing Australians. This Committee should recommend that the Government provide a clear and specific timeline for introducing the remaining reforms that out in the Attorney-General's Department Privacy Act Review Report and which were agreed to, or agreed to in principle by Government, within six months of the forthcoming federal election.

This submission focuses on certain parts of the Bill:

- HTI supports the statutory tort in Schedule 2 of the Bill, especially to the extent that it reflects the reform proposed by the Australian Law Reform Commission (ALRC) in its 2014 report.[1] However, HTI is concerned that the breadth of the exemptions undermines the efficacy of the tort, and we recommend tightening the broad exemptions in clauses 16, 17 and 18 of Schedule 2 to ensure a more targeted approach, in line with human rights and rule of law principles. HTI also recommends clarification of the consent defence in clause 8(1)(b) of Schedule 2, to ensure it only applies where consent is clear and unambiguous.

- HTI welcomes expanded powers for the Information Commissioner under clause 22 of Schedule 2, but recommends the broader role for the Privacy Commission envisaged by the ALRC—to investigate, and make declarations about, serious invasions of privacy—be included in the Bill.

- HTI welcomes the new transparency requirement in clause 88 of Schedule 1 of the Bill to inform individuals where automation is used in decision making that impacts them. To give this reform greater practical effect, HTI recommends the Bill also provide individuals with a right to request meaningful information about how substantially automated decisions with legal or similarly significant effect about them are made, in accordance with the Government's previous reform commitment.

HTI also recommends that the definition of 'personal information' be amended in the Bill, as agreed to in principle by the Australian Government in response to the Privacy Act Review Report.

[1] Australian Law Reform Commission (2014) *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123).

11 October 2024

List of recommendations

Recommendation 1

The Australian Government should commit to introducing the second tranche of legislation to reform the *Privacy Act 1988* (Cth) no later than six months after the forthcoming federal election. The second reform bill should incorporate the remaining recommendations that were agreed to, or agreed in principle, by the Government in its *Response to the Privacy Act Review Report*.

Recommendation 2

a. The broad exemptions in clauses 16, 17 and 18 of Schedule 2, applying to journalism, enforcement bodies and national security organisations, should be removed from the Bill.
b. The journalism exemption in clause 16 should be replaced with a defence that encompasses journalism in *the public interest*, such that the defendant will bear the onus of proving there was a public interest in the serious invasion of privacy that is prima facie unlawful under the elements of the statutory tort.
c. The defence for invasions of privacy that are 'authorised or required by law' in clause 8(1)(a) should be amended as follows:
    - The defence should be limited to activities that are '*expressly'* authorised by law.
    - Text should be added to clarify that:
        - enforcement bodies are covered by the defence only when they are conducting lawful investigations in respect of a serious crime, with independent authorisation;
        - intelligence agencies are covered by the defence only when they are conducting a lawful national security operation, with independent authorisation

Recommendation 3

Clause 8(1)(b) of Schedule 2, providing for a defence to the cause of action on the basis that express or implied consent had been given to the invasion of privacy, should be amended to require implied consent to be 'clear and unambiguous'.

Recommendation 4

The Bill should be amended to introduce a power for the Australian Privacy Commissioner to investigate complaints about serious invasions of privacy, and make appropriate declarations.

Recommendation 5

Clause 88 of Schedule 1 of the Bill should be amended to include a provision that would provide individuals with the right to request meaningful information about how substantially automated decisions with legal or similarly significant effects are made – as recommended by the Privacy Act Review report.

Recommendation 6

a. The Bill should be amended to expand the Privacy Act's definition of personal information, as recommended by the Privacy Act Review Report, to make clear

that personal information includes technical and inferred information (such as IP addresses and device identifiers) if this information can be used to identify individuals.

b. The Bill should be amended to expand the Privacy Act's definition of sensitive information, as recommended by the Privacy Act Review report, to clarify that sensitive information can be inferred from information that is not sensitive, to include genomic information and to define 'geolocation data' as personal information.

11 October 2024

Committing to a firm timeline for further privacy reform

In its response to the Privacy Act Review report, the Australian Government committed to implementing over 100 reforms to the Privacy Act.[2] While this Bill is a significant step forward, it does not address the vast majority of Privacy Act reforms the Government agreed to in whole or in principle. Importantly, the reforms proposed in this Bill will not address many of the most urgent, serious privacy concerns that need to be addressed in the context of new and emerging technologies.

In his Second Reading Speech, the Attorney-General stated the Bill is the first step towards more comprehensive privacy reform, and that a second tranche of reform is being developed.[3] This second tranche of amendments to the Privacy Act will be integral in ensuring the efficacy of the current Bill, not to mention the other changes needed to Australian privacy law. For example, the revised definition of 'personal information' and the other changes affecting automated decision making will have a significant impact on the operation of the provisions in this Bill.

Given the interconnected nature of these reforms, it would have been preferable to introduce a single Bill that implemented all of the Government's committed reforms to the Privacy Act. If, for practical reasons this cannot be done within the term of this Parliament, the Government needs to commit publicly to a clear and specific timeline for introducing the next bill. This timeline should be as expeditious as possible, noting that many of the reforms have been the subject of extensive public and broader stakeholder consultation – some going back almost two decades. Hence, this Committee should recommend that the Government commit to introducing the second reform bill to the Australian Parliament no later than six months after the forthcoming federal election.

Even with the improvements made in this Bill, legal protection for privacy in Australia remains woefully behind comparable jurisdictions. This leaves Australians with comparatively less adequate protections against invasive data collection practices, and other such privacy intrusions.[4] The outdated nature of the Privacy Act means that Australia is poorly prepared for the rise of technologies, such as artificial intelligence (AI), which rely on vast quantities of personal information, and which have led to an unprecedented scope and scale of collection, use, communication and storage of personal information. As these technologies evolve and expand, the deficiencies in the Privacy Act are creating an ever-larger problem for the Australian community and broader economy.[5]

Privacy law also underpins a range of other initiatives on the Australian Government's reform agenda. These include the federal Digital ID scheme; addressing disinformation and misinformation; AI law reform; cybersecurity; online safety and social media reforms; and consumer law protections. All of these reform areas are weakened by the

[2] Attorney-General's Department, *Government Response: Privacy Act Review Report* (Government Response, 28 September 2023).
[3] The Hon Mark Dreyfus KC MP, 'Second reading speech – Privacy and Other Legislation Amendment Bill 2024' *Attorney-General's Department* (Web Page, 12 September 2024) <https://ministers.ag.gov.au/media-centre/speeches/second-reading-speech-privacy-and-other-legislation-amendment-bill-2024-12-09-2024>.
[4] See, e.g., Denham Sadler 'Patient data used to train Aussie startup's AI' *Information Age* (Online) 24 September 2024 <https://ia.acs.org.au/article/2024/patient-data-used-to-train-aussie-startup-s-ai.html>.
[5] Attorney-General's Department, *Government Response: Privacy Act Review Report* (Government Response, 28 September 2023), 1.

lack of foundational, up-to-date privacy protections. Delays in implementing comprehensive privacy reforms undermine these parallel reform process, and increase market uncertainty, legal inconsistencies, gaps in protections, and unnecessary compliance burdens.

Outstanding urgent reforms

Some of the most urgent and important recommendations in the Government's own Privacy Act Review remain unimplemented. These include:

- *Fair and reasonable test*: This test would be a way of addressing the Privacy Act's over-reliance on consent, which is hugely burdensome on the individual, and an ineffective protection in practice. The fair and reasonable provision would require those collecting and using personal information to act fairly and reasonably regardless of whether the individual, whose personal information they are dealing with, has provided their consent.
- *Protections for biometrics and facial recognition technology*: Targeted reforms are needed to address high-risk technologies such as facial recognition technology, noting that this technology remains largely unregulated, and is capable of seriously breaching the human rights of Australians.
- *Small business exemption*: Approximately 94% of businesses in Australia are currently exempt from the Privacy Act due to the anomalous small business exemption, which leaves consumers exposed and unprotected.[6]

Recommendation 1

The Australian Government should commit to introducing the second tranche of legislation to reform the *Privacy Act 1988* (Cth) no later than six months after the forthcoming federal election. The second reform bill should incorporate the remaining recommendations that were agreed to, or agreed in principle, by the Government in its *Response to the Privacy Act Review Report*.

[6] Australian Law Reform Commission, *For your information: Australian privacy law and practice* (ALRC Report 108, August 2010) [33.44].

11 October 2024

Recommended amendments to strengthen the Bill

Statutory tort for serious invasions of privacy (Schedule 2)

The proposed statutory tort would create a cause of action for individuals who experience a serious invasion of privacy, addressing a significant gap in our civil law.

Subject to the relevant exemptions and defences, the tort would be made out where a defendant invaded a plaintiff's privacy by intruding upon the plaintiff's seclusion or misusing information that relates to the plaintiff, in circumstances where the plaintiff would have had a reasonable expectation of privacy and the invasion was intentional or reckless, and where the invasion was serious.[7] Where a defendant provides evidence that there was a public interest in the invasion of privacy, there is an onus on the plaintiff to satisfy the court the public interest was outweighed by the public interest in protecting the plaintiff's privacy.[8] A non-exhaustive definition of 'public interest' includes consideration of freedom of expression; freedom of the media; national security and the prevention and detection of crime and fraud; public health and safety; and the proper administration of government. [9]

The formulation of the tort imposes an appropriately high threshold; it does not, for example, include invasions that are negligent, but requires recklessness or intent to invade the plaintiff's seclusion or misuse of their information.

The tort is based on the model proposed by the Australian Law Reform Commission (ALRC model), in its 2014 report on *Serious Invasions of Privacy in the Digital Age.*[10] The ALRC model was thoroughly researched and tested through extensive consultation, and it was endorsed in the Privacy Act Review Report.

The Bill differs from the ALRC model in some key respects. HTI believes the broad exemptions in the Bill will unnecessarily weaken the scope of the tort's application, and the effectiveness of the tort as a tool to address serious infringements of privacy.

Exemptions

The Bill includes three broad exemptions for: (a) journalists, to the extent that the invasion of privacy involves the collection, preparation for publication or publication of journalistic material; (b) enforcement bodies, to the extent that the enforcement body reasonably believes that the invasion of privacy is reasonably necessary for one or more enforcement related activities; and (c) intelligence agencies.

HTI is concerned that these broad exemptions undermine the purpose of the tort in providing recourse for serious and unlawful infringements of privacy.

International human rights law, and rule of law principles, generally provide that any legal exemption or exception should flow from a specific, demonstrated justification based on the particular circumstance or activity in question, rather than merely the status of an organisation as operating within a context such as 'law enforcement,' 'intelligence' or 'journalism'.

[7] Privacy and Other Legislation Amendment Bill 2024, sch 2 cl 7.
[8] Privacy and Other Legislation Amendment Bill 2024, sch 2 cl 7(3).
[9] Privacy and Other Legislation Amendment Bill 2024, sch 2 cl 7(4)
[10] Australian Law Reform Commission *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123, 2014).

11 October 2024

Exemption for journalists (Sch 2, Cl 15)

The current wording of the journalism exemption would exclude *any* acts ostensibly done while developing 'journalistic material', regardless of the content or purpose of the journalism, including its merits as public interest journalism. This would exclude from coverage blatantly unlawful, even criminal, and unjustifiable infringements of privacy by journalists that are not in the public interest.

To provide further illustration, the tort in its current articulation would *not* cover:

- illegal phone hacking by a news corporation, as occurred during the News of the World phone hacking scandal in the United Kingdom;[11] or 'upskirting' photos taken of celebrities by a tabloid.
- a journalist maliciously publishing the home addresses and contact details of government officials. Doxxing would not fall within the scope of the tort if it occurred in the course of journalistic activities. However, doxing would be covered by the criminal provisions for doxxing offences in Schedule 3 of the Bill, where it meets the relevant criteria.

It would seem that it is precisely these types of infringements that the tort should apply to, as they are clear, serious infringements of privacy without principled justification.

Exemption for enforcement bodies (Sch 2, Cl 16) and intelligence agencies (Sch 2, Cl 17)

'Enforcement body' is said to have the same meaning as in the Privacy Act, which includes criminal law enforcement agencies such as police, and a range of other bodies at the state, territory and federal level with powers to issue civil penalties or sanctions, ranging from the Department of Home Affairs to Sports Integrity Australia.[12] The exemption applies when an enforcement body 'reasonably believes that the invasion of privacy is reasonably necessary for one or more enforcement related activities'. 'Enforcement related activity' is another broad term, which includes pursuing minor civil fines, and the prevention of minor crimes, such as speeding.[13]

It is relevant that there is a separate defence in clause 8(1) of Schedule 2 of the Bill for activities authorised by law – which would cover all *lawful* actions by enforcement bodies and national security organisations. The exemption for enforcement bodies could hypothetically cover *unlawful* actions by enforcement bodies, as long as the body 'reasonably believes the invasion of privacy is reasonably necessary'. This very low expectation of what the Bill deems to be proper behaviour by enforcement bodies, coupled with the extraordinary breadth of activities in respect of which enforcement bodies may claim this exemption, means that this exemption almost offers carte blanche to those bodies to flout the privacy protection in this new statutory tort.

Meanwhile *any* activity by intelligence agencies would be fully exempt from the scope of the tort, including activities conducted for malign or illegal purposes.

To provide further illustration, the tort in its current articulation would *not* cover:

- unlawful search and seizure by the Australian Tax Office, where it was 'reasonably believed it was reasonably necessary' to prevent potential tax avoidance

[11] See Lord Justice Leveson, *Report into the culture, practices and ethics of the press* (November 2012) <https://www.gov.uk/government/publications/leveson-inquiry-report-into-the-culture-practices-and-ethics-of-the-press>.
[12] *Privacy Act 1988* (Cth) s 6.
[13] Privacy and Other Legislation Amendment Bill 2024 sch 2 cl 6; *Privacy Act 1988* (Cth) s 6(1).

- illegal surveillance of Australian citizens by national security organisations due to their race, religion, sexuality or political beliefs.

It is not to the point that affected individuals may be able to take action against the relevant enforcement bodies under other legislation (such as anti-discrimination legislation, as in the second example above). The fact that they would be able to undertake such behaviour with impunity under the Privacy Act is unjustified.

If enforcement bodies or national security agencies unlawfully and seriously infringe a person's privacy, it is hard to argue on principled grounds that they should not be subject to the tort, and it would seem to contradict the Government's own stated intention in respect of the Bill. The Explanatory Memorandum states that the defences and exemptions are designed to 'recognise that *legitimate activities* of government may be privacy intrusive but are necessary and justifiable to ensure the proper administration of government.'[14]

Proposed amendments

Amendments to the exemptions provisions are necessary to ensure a more targeted approach, in line with human rights and rule of law principles. Under international human rights law, the right to privacy may be justifiably limited where the limitation is lawful and not arbitrary. In order for interferences not to be arbitrary, they must seek to achieve a legitimate aim (such as public interest, national security), and be reasonable, necessary and proportionate to achieving that aim.[15] Hence, as set out in greater detail below, it would be more appropriate to redraft this exemption as a limited defence, in circumstances where there is prior independent authorisation of the otherwise tortious conduction on the part of the enforcement body.

Journalism

As noted above, public interest journalism forms part of the elements of the tort. A specific exemption or defence was not considered necessary by the ALRC. The ALRC considered the balancing exercise now set out in clause 7(3) of Schedule 2 of the Bill

> is a more appropriate way to determine whether there is a public interest in the disclosure of the private information or the intrusion into an individual's seclusion. Expressly incorporating public interest into the actionability of a statutory cause of action will ensure that privacy interests are not unduly privileged over other rights and interests, particularly given that Australia does not have express human rights law protection for freedom of speech.[16]

HTI notes the significance of public interest journalism. Accordingly, if the tort is to retain an exemption or defence for journalism, for the avoidance of doubt, the scope should be narrowed so that it is clear it only applies to journalism that is in the *public interest*.

HTI notes that the Explanatory Memorandum states that the defendant bears the onus of proof for a defence, but it is silent as to how the onus of proof applies to exemptions. Preferably, the proposed exemption for journalism in the public interest should be re-framed as a defence with the onus of proof resting on the defendant.

Enforcement bodies and intelligence agencies

There is no need for a separate exemption for enforcement bodies and intelligence agencies that would otherwise be covered by the 'authorised by law' defence in

[14] Explanatory Memorandum Privacy and Other Legislation Amendment Bill 2024, 5. [Emphasis added]
[15] International Convention on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17; UN Commission on Human Rights, Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, UN Doc E/CN.4/1985/4 (28 September 1984).
[16] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123, 2014), 216.

Schedule 2 clause 8(1). The exemptions in clauses 16 and 17 should therefore be removed.

If, however, the exemptions remain in the Bill, the relevant clauses should be amended to better clarify the application of the exemptions.

First, clause 8(1) of Schedule 2 should be amended to clarify how this defence would apply to enforcement bodies and intelligence agencies. HTI proposes that the provision apply as follows:

- Enforcement bodies are covered by this defence if they are conducting lawful investigations in respect of a serious crime,[17] with independent authorisation. This wording would encompass authorisation through judicial warrants, and warrants issued by a judge or magistrate acting persona designata.
- Intelligence agencies are covered by this defence if they are conducting a lawful national security operation, with independent authorisation.

Secondly, the wording of this defence should be restricted to invasions of privacy required or *expressly* authorised by law. This would prevent arguments claiming that privacy interferences were merely *impliedly* authorised by law – for example, the use of spyware in devices that is not explicitly included in a warrant authorising some limited search activities.

Recommendation 2

a. The broad exemptions in clauses 16, 17 and 18 of Schedule 2, applying to journalism, enforcement bodies and national security organisations, should be removed from the Bill.
b. The journalism exemption in clause 16 should be replaced with a defence that encompasses journalism in *the public interest*, such that the defendant will bear the onus of proving there was a public interest in the serious invasion of privacy that is prima facie unlawful under the elements of the statutory tort.
c. The defence for invasions of privacy that are 'authorised or required by law' in clause 8(1)(a) should be amended as follows:
    - The defence should be limited to activities that are '***expressly***' authorised by law.
    - Text should be added to clarify that:
        - enforcement bodies are covered by the defence only when they are conducting lawful investigations in respect of a serious crime, with independent authorisation;
        - intelligence agencies are covered by the defence only when they are conducting a lawful national security operation, with independent authorisation.

Other amendments to improve the statutory tort

Consent defence (Sch 2 Cl 8(1)(b))

Schedule 2, clause 8(1)(b) of the Bill provides for a defence where 'the plaintiff, or a person having lawful authority to do so for the plaintiff, expressly or impliedly consented to the invasion of privacy'. This defence should be reworded, so that it applies to

[17] The definition of 'serious offences' in section 5D of the *Telecommunications Interception and Access Act* (Cth) could be adopted for this purpose.

express consent, and implied consent *only where consent was clear and unambiguous.* This will deter arguments where consent was not active or definitive on the facts – for example, where a plaintiff failed to respond to an email stating that certain measures would be taken if they did not explicitly opt out.

Recommendation 3

Clause 8(1)(b) of Schedule 2, providing for a defence to the cause of action on the basis that express or implied consent had been given to the invasion of privacy, should be amended to require implied consent to be 'clear and unambiguous'.

Role of the Office of the Australian Information Commissioner (Sch 2, Cl 22)

Schedule 2, clause 22 of the Bill provides that the Information Commissioner may, with leave of the court, intervene in proceedings or assist the court as amicus curiae. This is a narrower role for the OAIC than what was initially recommended by the ALRC. The ALRC model would have enabled the Privacy Commissioner to investigate complaints about serious invasions of privacy, and make appropriate declarations that would require referral to court for enforcement (in addition to functions enabling intervention in proceedings and amicus curiae.)[18] HTI recommends that this broader role be included in the Bill, as it would improve access to justice and access to remedies for individuals who have suffered serious breaches of privacy, and would make use of the Commissioner's expertise in handling privacy complaints.[19]

Recommendation 4

The Bill should be amended to introduce a power for the Australian Privacy Commissioner to investigate complaints about serious invasions of privacy, and make appropriate declarations.

Automated decision making (Schedule 1, Part 15)

Part 15 of Schedule 1 of the Bill introduces a requirement for entities to include information in privacy policies about the kinds of personal information used in, and types of decisions made by, computer programs that use personal information to make decisions that could reasonably be expected to significantly affect the rights or interests of an individual.

While this amendment would improve transparency regarding when automation is used in decision making, it is unlikely to have a significant practical impact. That is, providing additional information to individuals, such as in a privacy policy that an individual must consent to access a product or service, does little to support an individual seeking a review of an adverse decision.

Accordingly, clause 88 of Schedule 1 should also incorporate the recommendation in the Privacy Act Review report to provide individuals with a right to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. This recommendation was agreed to, without qualification, by the Government in its response.[20]

[18] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123, 2014) 310.
[19] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123, 2014) 310.
[20] Attorney-General's Department, *Government Response: Privacy Act Review Report* (Government Response, 28 September 2023) 11.

Including this recommendation in the Bill would provide substantive improvements for individuals subject to automated decision making. It would provide individuals with an opportunity to better understand how automated decisions affect them, which in turn enables them to take steps to exercise their rights in relation to the decision.

Recommendation 5

Clause 88 of Schedule 1 of the Bill should be amended to include a provision that would provide individuals with the right to request meaningful information about how substantially automated decisions with legal or similarly significant effects are made – as recommended by the Privacy Act Review report.

Support for the OAIC

HTI welcomes the expanded powers for the OAIC that are included in Part 2, and Parts 8 – 14 of Schedule 1 of the Bill. In order for these powers to be effective, the OAIC must be provided with sufficient resourcing to enable the exercise of these powers. The OAIC consistently faces extensive complaints backlogs and enforcement limitations due to underfunding.[21] These reforms will have very little impact without adequate capacity and means enabling the OAIC to enforce the law.

Additional reforms to include in the Bill

As noted above, it would have been preferable for this Bill to incorporate all of the Government's committed reforms to the Privacy Act. HTI accepts, with regret, that it is likely to be practically difficult to introduce those additional reforms in a Bill at this late point in the current parliamentary term. Nevertheless, HTI considers that the Bill could be amended without difficulty to include a smaller number of the Government's committed reforms, especially where those reforms will have a significant bearing on the Bill itself.

Amending the definition of 'personal information' and 'sensitive information'

'Personal information' is currently defined in s 6(1) of the Privacy Act to include 'information or an opinion about an identified individual, or an individual who is reasonably identifiable' whether that information or opinion is true or not.

This narrow definition fails to capture 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.

In its response to the Privacy Act Review Report, the Government agreed in principle to introduce amendments to the Privacy Act that clarify that 'personal information is an expansive concept that includes technical and inferred information (such as IP

[21] See, e.g., Brandon How, ''Extreme concern' about FoI, privacy complaint backlog' *Innovation Aus* (Online) 6 March 2022 <https://www.innovationaus.com/extreme-concern-about-foi-privacy-complaint-backlog/>.

addresses and device identifiers) if this information can be used to identify individuals.'[22]

Relatedly, designated categories of 'sensitive information' are outlined in section 6(1) the Privacy Act. Examples of sensitive information include information about a person's racial or ethnic origin, and biometric information. Sensitive information may only be collected with consent unless an exception applies, and more stringent requirements apply to its use.[23]

The current definition of sensitive information does not take into account the way that certain AI tools process information by categorisation and inference – enabling sensitive information to be derived from non-sensitive personal information. Nor does it take into account location data that can be used to track the precise geolocation of individuals.

The Government agreed in principle that the definition of sensitive information should be amended to include genomic information and to clarify that sensitive information can be inferred from information that is not sensitive information. The Government also agreed in principle that consent should be required for the collection of precise geolocation tracking data over time, and to consider further whether this should be included as a new sub-category of sensitive information.[24]

The definition of personal information is important: it articulates the scope of the Privacy Act regime. Relatedly, the definition of 'sensitive information' specifies a category of personal information that requires higher protections under the privacy regime. Accordingly, the Government should take the opportunity in this first reform bill to update the definitions of 'personal information' and 'sensitive information'. Including these amendments would underpin the other reforms in both the first and second tranches, since it relates to the scope of application of the Privacy Act as a whole.

Recommendation 6

a) The Bill should be amended to expand the Privacy Act's definition of personal information, as recommended by the Privacy Act Review Report, to make clear that personal information includes technical and inferred information (such as IP addresses and device identifiers) if this information can be used to identify individuals.

b) The Bill should be amended to expand the Privacy Act's definition of sensitive information, as recommended by the Privacy Act Review report, to clarify that sensitive information can be inferred from information that is not sensitive, to include genomic information and to define 'geolocation data' as personal information.

[22] Attorney-General's Department, *Government Response: Privacy Act Review Report* (Government Response, 28 September 2023) 5.
[23] *Privacy Act 1988* (Cth) sch 1.
[24] Attorney-General's Department, *Government Response: Privacy Act Review Report* (Government Response, 28 September 2023) 5-6.