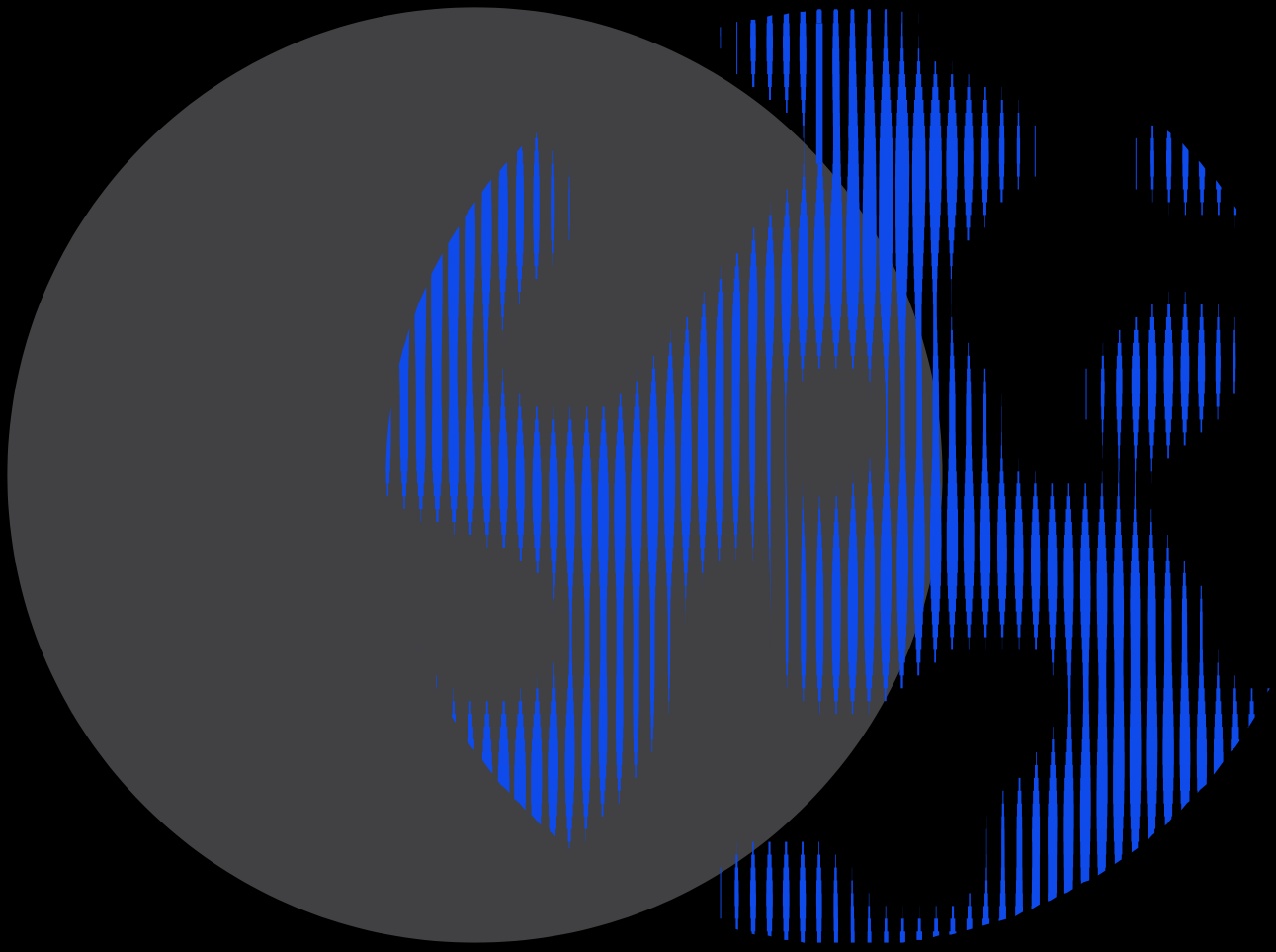
Human Technology Institute



Consultation on the exposure draft of the Privacy Amendment (Personal Data Protection) Bill 2026

Submission to the Attorney-General's Department

18 September 2026

18 September 2026

About HTI

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.

Authors: Sophie Farthing, Lauren Perry, Sarah Sacher and Professor Edward Santow

Contents

Executive summary 1

The Australian Government should implement committed reforms outlined in the exposure draft with amendments 4

- Fair and reasonable test 5
- Purpose limitation 8
- Exceptions for requirements to obtain consent for sensitive information 9
- Permitted general situations 10
- Collection notices 11
- Direct marketing 11
- Right to erasure 12
- OAIC powers 13

Amendments to the exposure draft to address high-priority issues 13

- Protections for biometric surveillance 13
- Direct right of action 15

Additional privacy law reforms 16

The OAIC must be sufficiently resourced to enforce the Privacy Act 17

Executive summary

HTI welcomes the exposure draft of the Privacy Amendment (Personal Data Protection) Bill 2026 (the exposure draft). If implemented, the exposure draft would modernise and strengthen the *Privacy Act 1988* (Cth) (Privacy Act). HTI supports the exposure draft, subject to some amendments outlined below.

Privacy reform is necessary and welcome

The exposure draft would introduce several key commitments made by the Australian Government in the whole-of-government response to the Attorney-General's Privacy Act Review Report (the AGD report). This once-in-a-generation reform would modernise our privacy law, giving greater confidence that AI and related technologies will not be used in breach of Australians' right to privacy and other related rights. It would also respond to public demand: 93 percent of Australians say that protecting personal information is important to them, and Australians rank privacy protection as their top priority for AI regulation.[1]

Many of the provisions in the exposure draft have been subject to extensive review and consultation over many years. A key reform is the introduction of the 'fair and reasonable' test, which is designed to combat the Privacy Act's over-reliance on consent, especially in the very common scenario that individuals are not in a position to provide genuine consent. Instead, this reform would require organisations and agencies to handle personal data responsibly, regardless of whether an individual appears to have provided their consent. Other welcome reforms include modernised definitions, including for 'personal information', which would enable the Privacy Act to give more effective protection against the use of personal data to profile and target individuals in the digital world.

Drafting amendments are needed, and key gaps remain

Reform of the Privacy Act is a singular opportunity. Hence, the Government must get the drafting of this bill right, so that the new measures operate effectively as intended.

HTI is concerned that the exposure draft includes amendments to the Privacy Act which were neither recommended by the AGD report nor committed to in the Government's response to that report, and which would reduce privacy protection. Those provisions – including exceptions, qualifications and scope limitations – derogate from the Government's reform commitments. Some of the provisions would also introduce new ambiguities regarding how the Privacy Act is to be interpreted and applied, as well as inconsistencies with related privacy protections in the *Digital ID Act 2024* (Cth) (Digital ID Act). HTI recommends those provisions be amended to avoid weakening protections in the Privacy Act, or otherwise making the Act more difficult for organisations, agencies and the community to apply.

Additionally, there remain outstanding gaps in the Privacy Act that must be addressed so that Australians are adequately protected, and privacy rights appropriately enforced. Until remaining Government commitments are implemented, Australians will remain vulnerable to misuse of their data by exempted entities, creeping surveillance, and harms associated with high-risk AI.

HTI proposes three categories of privacy reform. First, HTI recommends that the exposure draft be amended to improve the drafting of some key provisions, with a view

to better achieving the Government's stated intent, taking into account its existing reform commitments in the AGD Report.[2]

Second, the exposure draft should be amended to address some high-priority issues that would not otherwise by captured by the proposed reforms – including with respect to high-risk biometric and other surveillance technologies such as smart glasses and facial recognition technology.

Third, HTI urges the Department to address a small number of privacy-related reforms that appear to be outside the scope of the current reform process – for example, the removal of the anomalous small business exemption. If it is practically infeasible to address this third category of reform now, the Attorney-General should set out a timeline and process for making good on those remaining commitments.

Support for the regulator

HTI underlines the importance of resourcing the Office of the Australian Information Commissioner (OAIC) appropriately to support compliance with, and enforce, the Privacy Act. The OAIC cannot meet increasing demand in public complaints, fulfil enforcement objectives, nor adequately advise industry about their obligations, unless it is sufficiently funded.

Recommendations

1. **The exposure draft of the Privacy Amendment (Personal Data Protection) Bill 2026 should be passed with HTI's proposed amendments to ensure that the reform makes good on the Australian Government's prior commitments to privacy law reform.**

	Reform element	Recommended drafting amendment
1.1	Fair & reasonable test - *proposed new APP 3*.	The fair and reasonable test factors in proposed APP 3 of the Privacy Amendment (Personal Data Protection) Bill 2026 should be amended in line with HTI's proposed drafting. As amended, this would mean that the factors, which must be assessed in determining whether an organisation or agency has acted fairly and reasonably in handling personal information, would be: a) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency **(essential requirement)** b) whether a reasonable person would expect the collection, use or disclosure of the information in the circumstances c) whether the individual to whom the information relates has consented in relation to the collection, use or disclosure of the information d) the kind, sensitivity and amount of personal information being collected, used or disclosed e) proportionality assessment **(essential requirement)**, including consideration of: I. the impact on the privacy of the individual to whom the information relates, and any risk of harm to the

		individual arising from the collection, use or disclosure of the information *<u>Legislative note</u>: if the individual to whom the information relates is a child within scope of the Children's Online Privacy Code, that Code should be applied.* II. whether the restriction on privacy is not disproportionate to the likely benefit, taking into account safeguards that may mitigate risk of harm – such as transparency measures. *<u>Legislative note</u>: the benefit to the individual and any public benefit is given greater weight than the benefit to the APP entity.*
1.2	Purpose limitation – *repeal of current APP 6*.	Current APP 6 should be retained in the Privacy Act.
1.3	New exceptions for requirements to obtain consent for sensitive information – *proposed APPs 4.3 and 4.4*.	a) The proposed definition of 'publicly available document' in Item 1 of the Privacy Amendment (Personal Data Protection) Bill 2026 should be amended to exclude information where there is a 'barrier to access'. b) Proposed APP 4.3(d) should be deleted from the Bill.
1.4	Permitted general situations – *Item 17 (replacement of s 16A)*	a) Proposed wording changes to PGS table Item 2, column 3, should be clarified via a legislative note. The note should state that 'serious wrongdoing in this context is behaviour that amounts to serious misconduct, and would include where an entity suspects a person is exploiting a customer's vulnerability, or misusing enduring power of attorney for personal gain.' b) The words 'for sensitive information' should be deleted from proposed PGS table Item 1, column 3.
1.5	Notice requirements – *proposed APPs 5.1 and 5.3.*	The list of matters for notice requirements in APP 5.2 should be retained in the Privacy Act.
1.6	Direct marketing – *proposed APP 7.*	a) The proposed exception for ad-supported services should be deleted from the exposure draft, or otherwise significantly narrowed, to retain the integrity of the new digital marketing provisions. b) Current APP 7.6(e) should be retained in the Privacy Act.
1.7	Right to erasure – *proposed*	The qualification in proposed APP 14 that the right to erasure only applies to 'large digital platforms' should be deleted from the Privacy Amendment (Personal Data Protection) Bill 2026.

	schedule 4, part 2.	
1.8	New OAIC powers – *TBD.*	Proposals for new powers and processes for the OAIC should be implemented in the Privacy Amendment (Personal Data Protection) Bill 2026, and expanded to include a power for the OAIC to issue substantiation notices.

2. **The Australian Government should further amend the Privacy Amendment (Personal Data Protection) Bill 2026 to include:**

   a) **a requirement that the Privacy Commissioner develop a code on biometric and other surveillance technologies, modelled on s 26GC in the current Privacy Act**

   b) **a direct right of action where a regulated entity breaches the Australian Privacy Principles.**

3. **The Australian Government should implement outstanding privacy reform commitments prior to the next Federal election.**

4. **The Australian Government should make provision to resource the OAIC adequately to ensure that new and existing privacy protections are appropriately understood and enforced.**

The Australian Government should implement committed reforms outlined in the exposure draft with amendments

The exposure draft introduces a range of reforms directly recommended by the AGD report. HTI welcomes those reforms. However, some provisions of the exposure draft would significantly derogate from the Government's commitments, or introduce new ambiguities into the Privacy Act.

Additionally, some of these new provisions would lead to problematic inconsistencies with the Digital ID Act. When the Government introduced the Bill that became the Digital ID Act, it recognised that it could not rely only on the Privacy Act to protect Australians from privacy harms. As the Finance Minister acknowledged at the time, additional privacy protections were necessary to 'meet community expectations'.[3] Hence, the Digital ID Act contains an entire division that uplifts privacy protections in that digital ID context, in anticipation of upcoming Privacy Act reforms, including some based directly on AGD Report recommendations.

Because the exposure draft deviates from some of the AGD Report reforms in important ways – including with respect to its approach to sensitive information – this would cause unnecessary complexity and confusion for APP entities that must comply with both the general Privacy Act requirements and those that apply to the more specific digital ID context. For individuals, this would result in different levels of privacy protection - without any principled basis. In other words, it would take a problem (different privacy protections in the Privacy and Digital ID Acts) and convert it from a temporary to a permanent one.

HTI therefore recommends that the exposure draft be amended to bring it in line with the relevant provisions in the Digital ID Act and the Government's prior commitments.

HTI's proposed amendments are outlined in the following sections, and in the table on pages 2-4.

Other reforms should be passed without amendment, including the following welcome and significant proposals.

Welcome reforms that should be passed without amendment

Definitions of personal and sensitive information (proposed ss 6FD, 6FE and 6FF): These updated definitions would broaden the scope of the Privacy Act regime to encompass the ways in which data can be used to identify, profile and target individuals in the digital world.

Definition of consent (proposed s6AAB): The updated definition of consent would serve to improve the quality of consent obtained from individuals, in line with AGD Report recommendations.

Strengthened requirements for data deletion, data security and data breach notification (proposed schedule 3): The exposure draft includes a range of proposed provisions that would introduce new requirements for entities to take steps to protect personal data; proactively consider whether to destroy data that is no longer needed; and take reasonable steps to either destroy or de-identify unneeded information; as well as strengthened obligations on entities to respond to and contain data breaches. This will assist in preventing and responding to misuse and interference with data and poor data handling practices that cause harm to individuals.

Requirements for trading of personal information (proposed APP 4.2): The inclusion of provisions relating to the trading of personal information would cover a broad range of arrangements in which personal information is disclosed as part of an exchange, with related consent requirements, implementing an AGD Report recommendation.

Recommendation 1

The exposure draft of the Privacy Amendment (Personal Data Protection) Bill 2026 should be passed with HTI's proposed amendments to ensure that the reform makes good on the Australian Government's prior commitments to privacy law reform.

HTI's proposed amendments are elaborated below and summarised in the Table on pages 2-4.

Fair and reasonable test

HTI supports the inclusion of proposed APP 3, which would introduce a new provision that requires APP entities to handle personal information fairly and reasonably. This reform could:

- combat the inappropriate reliance by APP entities on consent, and especially non-genuine consent, in ways that nullify or reduce an individual's privacy law protections. The reliance on consent is both burdensome on the individual and often an ineffective protection on its own. As the 2026 OAIC survey found, 68% of Australians feel like they have 'no genuine choice' but to share their personal information when engaging with entities.[4]
- ensure that APP entities give greater weight to the privacy rights of individuals before handling their personal information. This would shift the burden from individuals who cannot practically manage or control how their data is used; to organisations who would be required to handle data responsibly.

This reform was thoroughly tested through the AGD review process, and would reflect approaches taken in comparable jurisdictions such as the European Union and the United Kingdom, supporting interoperability with those jurisdictions.[5]

However, it is necessary to make some amendments to the drafting of factors in the fair and reasonable test so as meaningfully to improve privacy protections for Australians.

Amendments to individual fair and reasonable factors

Problems with articulation of fair and reasonable factors

There are three problems with the drafting of the fair and reasonable provision in the exposure draft.

First, proposed new APP 3.2(b) states that, in determining whether it would be fair and reasonable to collect use or disclose personal information, an APP entity must consider 'whether the collection, use or disclosure of the information *relates to* one or more of the APP entity's functions or activities'. This differs from the Government's original proposed wording which was 'whether the collection, use or disclosure is *reasonably necessary* for the functions and activities of the organisation or is reasonably necessary or *directly related* for the functions and activities of the agency' (emphasis added).[6]

This factor addresses whether an APP entity has a legitimate purpose for handling the personal information in the first place. APP entities should have a good reason for handling an individual's personal information – hence the original wording asks whether this is *reasonably necessary* for an organisation's functions or activities (and a similar standard for government agencies).

If an APP entity could satisfy this factor merely because the personal information handling *relates to* its functions/activities, it would allow significantly more personal data collection and use. For example, the exposure draft wording would allow a real estate agent to gather personal data from renters, to determine whether they could afford to pay higher rental fees, because this would be related to the service the agent is providing. But that rationale wouldn't satisfy the factor under the original wording, because such information isn't *reasonably necessary* to provide the rental service. The new wording would therefore be a step backwards.

APP entities also already understand and implement the 'reasonably necessary' requirement, as a similar obligation currently applies under APP 3 (and would otherwise be repealed by the exposure draft) – this familiarity would usefully assist in the transition to the fair and reasonable test if the same wording were adopted.

Second, proposed new APP 3.2(e) asks whether the individual is 'provided with genuine choice' in relation to the collection, use or disclosure of information. HTI recommends that proposed APP 3.2(e) be redrafted to require consideration of whether the individual has given consent. Merely giving the opportunity for genuine choice, without assessing whether someone has taken that opportunity, would re-introduce one of the problems with sham consent, which this Bill is trying to address.

In any case, the AGD Report proposed that the fair and reasonable test would apply in *addition* to consent requirements. The exposure draft includes a new definition for consent, which HTI welcomes. This definition would help improve consent processes, which are necessary but not sufficient on their own.

Third, the proposed fair and reasonable test excludes one original factor from the AGD Report – a requirement for entities to consider 'the kind, sensitivity and amount of information being collected, used or disclosed'. The amount and nature of personal data being handled are directly relevant to whether the APP entity is acting fairly and reasonably. For example, collecting more personal data increases the risk to the

person's privacy, and this should be justified. Hence, this consideration should be included either as a standalone fair and reasonable factor as originally intended, or as an explicit element of the proportionality factor (proposed APP 3.2(f)).

Other minor drafting clarifications

The proportionality factor (proposed APP 3.2(f)) could be more clearly articulated to reflect the proportionality test under international human rights law that it is intended to implement. A legislative note should clarify that when considering whether the impact is proportionate to the benefit, benefits to the individual, and public benefits, should be weighted more heavily than benefits to the APP entity. This note would prevent confusion regarding the purpose of the fair and reasonable test, and the role of the Privacy Act as a whole – that is, the Privacy Act exists to protect the human right to privacy in Australia, in line with Australia's international law obligations. The right to privacy is intended to co-exist with industry's legitimate commercial activities, but that co-existence should not involve unjustified restrictions on the right to privacy.

Proposed APP 3.2(g) requires consideration of the best interests of the child as a primary consideration. This factor is largely addressed through the Children's Online Privacy Code – which could be cross-referenced in the test.

Some fair and reasonable factors should be essential requirements, and the test should be streamlined

In the current exposure draft, while each of the proposed fair and reasonable factors must be considered, none is essential. In other words, where an APP entity fails to satisfy the conditions in a particular factor, this would not necessarily mean that the APP entity is breach of the fair and reasonable test. Even if the APP entity fails to satisfy the conditions in more than one of the factors, it will not necessarily fall foul of the test as a whole. This could have the unintended consequence of encouraging poor compliance with this particular privacy principle.

To combat that risk, HTI recommends that some of the fair and reasonable factors be classified as essential requirements. This would better encourage APP entities to act conscientiously to comply with the most important baseline expectations in acting fairly and reasonably when handling personal information; and it would prevent unintended weakening of existing Privacy Act requirements. HTI recommends that proposed APP 3.2(b) (reasonably necessary' as redrafted above), and APP 3.2(f) (proportionality) be treated as essential requirements. This would mean that entities would be required to both consider and take active steps to address those essential factors when collecting, using or disclosing data. This would capture core steps for rights assessments under international human rights law, upon which the fair and reasonable test is based.

The test should also be streamlined. The collective drafting changes to the test in the exposure draft, including new factors introduced into the test post-AGD Report, have led to the factors becoming somewhat duplicative – they should be condensed, and re-ordered into a more logical sequence, so that the test is simpler for APP entities to apply in practice.

Taking into account HTI's above suggested amendments, HTI proposes that the test be re-drafted to contain the following factors:

a) Whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency (**essential requirement**)

> *This would incorporate proposed factor 3.2(d): whether the purpose for which the information is being collected, used or disclosed could be met*

by collecting, using or disclosing less information, or information that is not personal information

b) Whether a reasonable person would expect the collection, use or disclosure of the information in the circumstances

c) Whether the individual to whom the information relates has consented in relation to the collection, use or disclosure of the information

d) The kind, sensitivity and amount of personal information being collected, used or disclosed

e) Proportionality assessment (**essential requirement**), including consideration of:

I. the impact on the privacy of the individual to whom the information relates, and any risk of harm to the individual arising from the collection, use or disclosure of the information

Legislative note: if the individual to whom the information relates is a child within scope of the Children's Online Privacy Code, that Code should be applied.

This would incorporate 3.2(g): best interests of the child

II. whether the restriction on privacy is not disproportionate to the likely benefit, taking into account safeguards that may mitigate risk of harm – such as transparency measures.

Legislative note: the benefit to the individual and any public benefit is given greater weight than the benefit to the APP entity.

This would incorporate proposed factor 3.2(c): *whether the APP entity is transparent about the means and the purposes of the collection, use or disclosure of the information*

Recommendation 1.1

The fair and reasonable test factors in proposed APP 3 of the Privacy Amendment (Personal Data Protection) Bill 2026 should be amended in line with HTI's proposed drafting.

Purpose limitation

The exposure draft would repeal current APP 6, which was not recommended by the AGD Report. Currently, APP entities cannot use or disclose personal information for a secondary purpose, unless consent has been given or specified conditions met. The repeal of APP 6 would remove this requirement – and it is not otherwise captured by the fair and reasonable test provisions.

Purpose limitation is a vital privacy protection, because it sets a default restriction on how personal information can be handled, based on an APP entity's most relevant justification – its 'primary purpose'. Handling personal information for a secondary purpose should require more specific justification – as the Privacy Act currently provides.

This protection is particularly important in our data-driven economy, where there are many avenues and incentives for repurposing data originally collected for more specific or innocuous purposes. For example, data collected through a customer rewards program can be used for purposes such as targeted advertising and/or surveillance pricing measures; or sold to data brokers for financial gain. Data collected for a public

employment service could be used for intrusive government surveillance, or to train AI systems.

Removing this protection would weaken the Privacy Act. Therefore, current APP 6 should be retained.

Recommendation 1.2

Current APP 6 should be retained in the Privacy Act.

Exceptions for requirements to obtain consent for sensitive information

The Exposure Draft proposes two new exceptions to consent requirements for the collection of sensitive information in proposed APP 4.3 and 4.4. These exceptions were not recommended in the AGD Report, and HTI recommends that both exceptions be removed, or at least more narrowly scoped.

Proposed APP 4.3(b) would create an exception where personal information is collected from a publicly-available document. Item 1 states that this includes documents that are available subject to a 'barrier to access', such as a fee or account registration, provided the barrier could be overcome by an ordinary member of the public.

This exception could apply to, for example, sensitive information obtained from: a data broker upon payment of a fee; criminal records databases; private social media pages or forums for people with protected attributes – such as support groups for people with mental health conditions. Despite the 'barrier to access' such information should not reasonably be considered 'publicly available', especially in the modern era when personal information is commonly held or shared for specific purposes online, albeit behind 'barriers'. Sensitive information should not be used or disclosed without an individual's awareness or consent – and doing so could cause significant harm. If this exception is to be retained, the definition of publicly-available documents should be amended to *exclude* information where there is a 'barrier to access'.

Proposed APP 4.3(d) would provide that consent is not required where collection is strictly necessary to provide or deliver a good or service explicitly requested by an individual, and where the good or service cannot be provided in a less privacy intrusive manner. It is possible that there is drafting error in the exposure draft – as clause (d) may be intended to be read with clause (c) and thus be limited to not-for-profit organisations – but this is not the plain meaning of the text, nor is it explained as such in the Consultation Paper. This point needs further clarification.

If proposed 4.3(d) *is* intended as a standalone exception, HTI's view is that it should be deleted. It is no less important for individuals to know and consent to the use of their sensitive information, regardless of whether they've requested the relevant good/service or not. This has long been the status quo approach in the Privacy Act, and there is no apparent justification as to why this should change.

As noted above, if these exceptions were introduced, they would be inconsistent with higher standards for sensitive information contained in ss 45, 46 and 48 of the *Digital ID Act 2024* (Cth).

Recommendation 1.3

a) **The proposed definition of 'publicly available document' in item 1 of the Privacy Amendment (Personal Data Protection) Bill 2026 should be amended to exclude information where there is a 'barrier to access'.**

b) **Proposed APP 4.3(d) should be deleted from the Bill.**

Permitted general situations

Item 17 of the exposure draft would replace s 16A, which sets out permitted general situations (PGS). Changes to PGS provisions were not recommended by the AGD Report, and may have the effect of reducing the limited protections that currently apply to PGSs under the Privacy Act – this is particularly concerning in the context of high-risk AI and emerging technologies like biometric surveillance devices.

In a PGS, Privacy Act requirements to obtain consent for sensitive and personal information do not apply. PGSs arise in exceptional situations – such as where there is risk to life, or serious misconduct (PGS 1, 2). PGS exceptions can, and are, relied upon to introduce high-risk technologies, such as facial recognition technology in retail and policing contexts.[7] While personal and sensitive data handling in the context of a PGS generally involves high risks of harm and human rights impacts (such as loss of liberty, discrimination or restrictions on freedom of association), the Privacy Act allows for carve outs from some Privacy Act obligations that are otherwise applicable – which is why the exception should remain narrowly constrained, with a high bar for application.

Drafting changes to PGS 2

The exposure draft would amend PGS 2 to replace 'misconduct of a serious nature' with 'wrongdoing of a serious nature' as the basis for a PGS being on foot. The Consultation Paper explains that this is intended to be 'broader than misconduct', and include conduct by a person acting in a private capacity – such as in cases where an entity suspects a customer may be experiencing financial abuse.[8] This term is not defined in the draft, and it is not clear on its face how broadly the term 'serious wrongdoing' may apply, nor how it differs from serious misconduct.

HTI recommends that the Bill define 'wrongdoing' as behaviour that amounts to serious misconduct, with a statutory note to make clear that wrongdoing in this context would include where an entity suspects a person is exploiting a customer's vulnerability, or misusing enduring power of attorney for personal gain.

Drafting changes to PGS 1

Currently PGS 1 applies only when 'it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure' of both personal and sensitive information. The exposure draft would alter this wording, so that this limb only applies to sensitive information. This change is not flagged in the Consultation Paper, despite broadening the scope of the PGS for no apparent principled reason.

HTI recommends that the drafting of PGS table, Item 1 column 3 should delete the words 'for sensitive information' so that the exception is not widened beyond its current articulation in the Privacy Act.

Recommendation 1.4

a) **Proposed wording changes to PGS table Item 2, column 3, should be clarified via a legislative note. The note should state that 'serious wrongdoing in this context is behaviour that amounts to serious misconduct, and would include where an entity suspects a person is exploiting a customer's vulnerability, or misusing enduring power of attorney for personal gain.'**

b) **The words 'for sensitive information' should be deleted from proposed PGS table Item 1, column 3.**

Collection notices

HTI supports clarification regarding the form of notices informing of the collection of personal information in proposed APP 5.3, which directly implements an AGD Report recommendation. However, the AGD Report also recommended that this reform be introduced alongside the existing list of matters to be included in notices, outlined in APP 5.2.[9] Instead, these matters would be substantially reduced by proposed APP 5.1.

Thorough notices are important for assisting individuals to understand how their data is being used, make informed choices about whether and how to engage with a service, and enforce their rights. The OAIC has emphasised this message on a number of occasions, and the AGD Report reflected this reasoning.[10] Retaining APP 5.2 does not equate to overly lengthy or complex notices – as only relevant matters which serve the purpose of informing the individual in the circumstances need to be addressed in a notice. HTI therefore recommends that notice content requirements in APP 5.2 be retained.

Recommendation 1.5

The list of matters for notice requirements in APP 5.2 should be retained in the Privacy Act

Direct marketing

HTI welcomes new requirements in proposed APP 7 for digital marketing, including for opt outs, which would apply in addition to the fair and reasonable test. However, these provisions are significantly undermined by a broad exception for 'ad-supported services' – which should be removed.

Ad-supported services exemption

The exposure draft defines 'ad-supported services' in proposed APP 7.6 as entities for whom the 'marketing communications to individuals who use the service is itself a source of revenue for the organisation'. If individuals opt-out of these services, proposed APP 7.5 would enable them to offer the service 'on terms that differ from the terms on which the service or element is offered to individuals who receive direct marketing, as long as the different terms provide the individual with genuine choice to continue.'

The direct marketing provisions apply to targeted advertising that uses personal information – including in ways that are manipulative, opaque and exploitative. They do not capture advertising that does not rely on personal information. There should naturally be a high bar for advertising that relies on personal information, especially given the risk of harm is high.

The proposed exception for ad-supported services would permit a wide array of organisations and platforms, including social media services, news media, and gaming apps, to offer a worse service for people who opt-out of direct marketing using their personal information. This would not create conditions for people to provide genuine consent, and could indirectly enable the kinds of manipulative practices that these new protections are intended to prevent.

This exception was not recommended by the AGD Report – in fact, the AGD Report recommended 'unqualified rights' to opt out of direct marketing.[11] There may be cases where it is reasonable for ad-supported services to offer an alternative experience for those who opt out of direct marketing – for example, customers that *do not* opt out of direct marketing on a shopping site may receive personalised recommendations or

feeds; customers who *do* opt out would not have access to this feature. However, the exposure draft contains a wider exception than this. Its breadth would undermine the protective intent of the provisions. If the exception cannot be appropriately narrowed, it should be removed.

As with the sensitive information exceptions discussed above, these provisions would also be inconsistent with privacy protections in the Digital ID Act which generally prohibit the use or disclosure of personal information for marketing purposes, subject to very limited exceptions.[12]

Proposed repeal of APP 7.6(e)

Current APP 7.6(e) facilitates individuals being able to request the source of information used for direct marketing. An equivalent position does not appear in the new drafting of APP 7. Individuals should be able to retain the option to request the source of information used to make direct marketing communications.

Recommendation 1.6

a) **The proposed exception for ad-supported services should be deleted from the exposure draft, or otherwise significantly narrowed, to retain the integrity of the new digital marketing provisions.**

b) **Current APP 7.6(e) should be retained.**

Right to erasure

HTI supports a right to erasure. The current drafting in proposed Schedule 4, Part 2 would allow the right to be exercised only against 'large digital platforms'. This should be redrafted as a general right to erasure applicable to all APP entities.

The AGD Report proposed a general right to erasure, allowing individuals to have their personal information erased, which would also address third parties who hold data. That approach mirrors laws in jurisdictions such as the EU, UK and California.[13] A general right to erasure would enable individuals to exercise more control over their data – including where their data has been used without their consent, where they have withdrawn consent, or where their data is being used in ways that cause harm. On the whole, a general right to erasure would help to address the power imbalance between individuals and the APP entities that hold their personal information, while encouraging better data minimisation and deletion practices by entities. This in turn reduces risks associated with, for example, data breaches.[14]

The exposure draft would allow this right to be exercised only as against 'large digital platforms' (with gross annual revenue of $500 million or more, or with 2.5 million or more average monthly end users). There is no clear practical or principled justification for this restriction to the right to erasure. It would mean that Australians would continue to be denied the right to request that their data to be erased in circumstances such as where:

- an individual's personal data has been collected for a gym membership that they no longer use, yet they continue receiving insistent updates and marketing for a range of gyms owned by the parent company and related products;
- photographs of a teenager are used to publicly promote a dermatologist, but as an adult, they no longer consent to their data continuing to be used in this way;
- an individual suspects that a real estate platform is using sensitive information about them to inform adverse decisions regarding rental applications, where that information is not strictly necessary for the platform's operation.

The qualification that the right only applies to 'large digital platforms' should therefore be deleted.

Recommendation 1.7

The qualification in proposed APP 14 that the right to erasure only applies to 'large digital platforms' should be deleted from the Privacy Amendment (Personal Data Protection) Bill 2026.

OAIC powers

HTI supports proposals for new powers and processes that would enable the OAIC to more effectively enforce the Privacy Act. HTI also recommends that the OAIC be granted the power to issue substantiation notices as part of this package.

Substantiation notices are an important power for regulators in the digital age. When substantiation notices are issued, a person must produce information or documents capable of substantiating representations made by that person. This power would be especially useful in respect of products and services that rely on AI, because it can be very difficult for regulators to determine how such products and services use personal information – particularly in the initial stages of an investigation.

Providing the OAIC with this power would align it with other Australian regulators. In 2009, the ACCC and ASIC were both conferred the power to issue substantiation notices to protect consumers because 'the lack of an ability to quickly and easily require information to substantiate claims made in representations by businesses' was a 'key gap in the powers of the ACCC and ASIC'.[15]

Recommendation 1.8

Proposals for new powers and processes for the OAIC should be implemented in the Privacy Amendment (Personal Data Protection) Bill 2026, and expanded to include a power for the OAIC to issue substantiation notices.

Amendments to the exposure draft to address high-priority issues

There remain outstanding gaps in the Privacy Act that must be addressed so that Australians are adequately protected, and privacy rights appropriately enforced. HTI recommends that two priority reforms be included in the exposure draft – each would substantively address serious harms affecting Australians, and would require simple and straightforward amendments to the existing exposure draft.

Protections for biometric surveillance

HTI welcomes the Government's recognition of the immediate and significant threat to privacy posed by biometric and other surveillance technologies.

These types of privacy-invasive technologies have various functions and capabilities, which can be combined in a single product or service:

- *biometric scanning technologies* capture and process records of biometric information, such as a person's face, iris, palm, signature or voice (for example, when you scan your thumb to log into a work computer)
- *facial recognition technology (FRT)* uses biometric data from scanning human faces to verify who someone is (1:1 matching), identify a particular individual from a larger database (1:many matching) and/or analyse, characteristics about

a person (for example, having your face scanned at an airport immigration booth to verify your identity)

- *surveillance technologies* include devices, software or systems which can capture or record audio, video, location or other data (including biometric data) to obtain or infer particular information about a person, place or object; or to control or alter behaviours.

There has been rapid expansion of FRT and surveillance technologies across the public and private sectors. Live FRT is currently being trialled by Western Australian police and used by sporting venues to replace conventional ticketing systems,[16] EFTPOS machines are adopting 'pay with your face' technologies,[17] and major retailers are testing and implementing FRT in their stores.[18] Increasingly popular and low-cost smart glasses have sparked intense public concern, and are capable of being used for many harmful and criminal purposes, including stalking and harassment.[19] Many smart glasses products also have the capacity to embed FRT in their operation, or could do so in future. [20]

HTI has long warned of the significant human rights risks – including to the right to privacy – of technologies that enable the capture of biometric information. Unlike other traditional surveillance technologies, such as CCTV, emerging biometric and surveillance technologies (especially those which capture audio, images or video) can remotely and covertly capture sensitive information without an individual's knowledge. If left unchecked, the proliferation of these types of technologies raises a real risk of mass surveillance.

The Privacy Act, including with the amendments proposed in the exposure draft, largely fails to address the serious implications of these technologies for the right to privacy. A dedicated legislative response is urgently required.

Urgent law reform to protect privacy

HTI has previously outlined a model law for FRT that would introduce the necessary safeguards to protect the privacy of individuals, and which would appropriately balance positive innovation with the risk of harm posed by FRT.[21] HTI's model law would require entities that develop or deploy FRT systems to undertake a facial recognition impact assessment with incremental legal obligations applied depending on the assessed risk level. In particularly high-risk cases, under HTI's FRT model law, there would be restrictions or prohibitions on the use of FRT.

Development of an APP Code for biometric and surveillance technologies

HTI's primary position remains that the Government should introduce legislation along the lines of the HTI model FRT law. However, in the event that the Government opts not to do so, at least in the short term, HTI recommends the Privacy Act be amended to mandate the Privacy Commissioner to develop an APP Code for biometric and surveillance technologies under Division 2 of the Privacy Act. This would require a new clause to be inserted, which should be modelled on s 26GC of the Privacy Act.

A code for biometric and surveillance technologies should set out how one or more of the APPs should be applied or complied with by the developer or deployer of any biometric or surveillance technology. It should apply to any APP entity that develops, offers, markets, distributes, deploys or uses biometric and surveillance technologies in Australia. The code should be developed within 12 months, based on consultation with the public and relevant regulators such as the eSafety Commissioner.

To address the rapidly expanding availability and use of surveillance technologies by individuals, such as the use of low-cost smart glasses, HTI recommends the Code also

apply to an individual using a device that incorporates technology that can record video or audio, either covertly or overtly, without obtaining informed consent of the subject. Application of the Code to individuals (ie, beyond APP entities) would require ancillary amendment to clarify that certain provisions in the Code apply also to individuals.

A Code could apply to a range of activities, such as:

- an Australian start-up developing emotion recognition software
- commercial entities deploying FRT to manage in-store safety and security
- an individual video-recording another individual using a smart, wearable device, without obtaining that person's consent.

In addition, the Code could incorporate commitments already made by the Government in response to the Privacy Act Review, including banning small businesses from collecting biometric information for use in FRT; [22] and the conduct of a privacy impact assessment for activities with high privacy risks (including FRT) prior to the commencement of that activity. [23]

An APP Code presents a proportionate, flexible and immediate response

Mandating the development of a Code under the Privacy Act would support the adoption of a proportionate, risk-based approach to an immediate threat to personal privacy. An APP Code is a flexible regulatory tool that would safeguard the personal and sensitive information of individuals. A code could also consider how to permit and support privacy-compliant positive use cases of biometric and surveillance technology – such as enabling an individual with a disability to use the technology as an accessibility aide or tool, or an individual taking photos of family and friends with a smart, wearable device without receiving explicit consent. The Code could also provide guidance and impose obligations on law enforcement and national security agencies regarding their proposed use of biometric and surveillance technologies. This could be achieved via adoption of the principles established in the 'FRT in Enforcement Regime' set out in HTI's model law.

A code would also sit alongside, and support, other applicable regulatory activity, such as the incorporation of Safety by Design principles developed by the eSafety Commissioner.[24] A code would also go some way towards addressing regulatory gaps, for example: where it is unclear whether the behaviour is unlawful under other laws like criminal codes or surveillance acts, or where the conduct causes harm but may not meet the threshold of seriousness for the statutory tort for serious invasions of privacy.

Recommendation 2

The Australian Government should amend the Privacy Amendment (Personal Data Protection) Bill 2026 to include a requirement that the Privacy Commissioner develop an APP Code on biometric and other surveillance technologies, modelled on s 26GC in the current Privacy Act.

Direct right of action

Where a company or government agency, covered by the Privacy Act, breaches the Australian Privacy Principles, it be can be difficult and very slow for an individual to enforce their rights via a relatively small regulator, which has very limited resources. Australians do not have a right to enforce privacy breaches through Australian courts, which puts intense pressure on the regulator and limits their right to access justice when harmed.

HTI recommends the Privacy Act be amended to provide a direct right of action in respect of a breach of the APPs, to better enable individuals to seek remedies in the courts for privacy breaches, as per the AGD Report recommendation. Allowing individuals to apply directly to the courts for relief when their privacy is interfered with would improve the pathways available to uphold privacy rights under the Act, and would incentivise compliance by APP entities. This would bring Australia into alignment with jurisdictions such as the EU and New Zealand.[25] The introduction of this right also has overwhelming community support: the 2026 OAIC survey found that 88 percent of Australians were in favour of a right to seek compensation in court for breaches of privacy.[26]

Recommendation 3

The Australian Government should further amend the Privacy Amendment (Personal Data Protection) Bill 2026 to include:

a) **a requirement that the Privacy Commissioner develop a code on biometric and other surveillance technologies, modelled on s 26GC in the current Privacy Act**

b) **a direct right of action where a regulated entity breaches the Australian Privacy Principles**.

Additional privacy law reforms

The AGD should adopt a pathway to make good on the Albanese Government's other committed privacy law reforms. In particular, the Privacy Act includes several exemptions that leave Australians unprotected in everyday contexts.

The employee records exemption excludes the Privacy Act from regulating an employer's handling of personal data relating to the employment of its employees.[27] This exemption, combined with gaps in employment laws, mean that Australian workers are largely unprotected from harms related to worker surveillance. If this issue is not addressed through Privacy Act reform, it can be effectively dealt with through amendments to employment laws. HTI's March 2026 Snapshot Report, *Surveillance Creep*, described the alarming rise of tech-enabled worker surveillance in Australia and the inadequacy of our current laws.[28] HTI's forthcoming report, *Drawing the Line: tech-enabled surveillance of Australian workers* (October 2026) will set out a proposal to address this issue through practical and targeted amendments to the Fair Work Act.

The small business exemption excludes approximately 94% of businesses in Australia from compliance with the Privacy Act.[29] This anomalous exemption leaves consumers exposed and unprotected, and should be repealed. 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. Falling costs and increasingly easy access to new technologies like AI and surveillance technologies – including facial recognition technologies – mean that even small organisations may have a significant, scalable impact on the privacy of everyday Australians.

Generally, regarding all 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.

Recommendation 4

The Australian Government should implement outstanding privacy reform commitments prior to the next Federal election.

The OAIC must be sufficiently resourced to enforce the Privacy Act

New laws only protect people if they are adequately enforced. The OAIC is facing increasing demand: to illustrate, it received 11,800 matters in the 2025–26 financial year, compared to 7,717 received in 2024–25.[30] Despite this, the OAIC was allocated $36.576 million in the 2026-27 Federal Budget – down from $39.753 million in 2025-26, and representing an 8 per cent cut to the agency's departmental appropriation.[31]

The implementation of the exposure draft would serve to compound existing demand on the OAIC. In our data-driven world, Australians routinely experience privacy and AI related harms, and the OAIC must be in a position to respond appropriately. At the same time, businesses require guidance on how to comply with new provisions, which the OAIC is best placed to provide. New reforms should be packaged with increased funding for the OAIC so that they can continue to fulfil their remit.

Recommendation 5

The Australian Government should make provision to resource the OAIC adequately to ensure that new and existing privacy protections are appropriately understood and enforced.

---

[1] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey* (May 2026) 26 <https://www.oaic.gov.au/__data/assets/pdf_file/0023/264362/ACAPS-2026-Report.PDF>. Tech Policy Design Institute, *Earning Trust: Unlocking AI Adoption for Australians* (Policy Spotlight, May 2026) <https://techpolicy.au/earning-trust/>

[2] Australian Government, *Government Response: Privacy Act Review Report* (September 2023) <https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report>.

[3] Parliament of Australia, *Parliamentary Debates,* Senate, 30 November 2023, 6281 (Senator Katy Gallagher).

[4] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey* (May 2026) 4 <https://www.oaic.gov.au/__data/assets/pdf_file/0023/264362/ACAPS-2026-Report.PDF>

[5] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation) Art 6.

[6] Attorney-General's Department, *Privacy Act Review Report* (February 2023) 8 (Proposal 12.2) <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>.

[7] See, e.g. *Bunnings Group Limited and Privacy Commissioner* (Guidance and Appeals Panel) [2026] ARTA 130 (4 February 2026).

[8] Attorney-General's Department, *Privacy Reform – Consultation Paper* (August 2026) 19.

[9] Attorney-General's Department, *Privacy Act Review Report* (February 2023) 99 (proposal 10.2) <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>

[10] See, e.g., *Commissioner Initiated Investigation into Medmate Australia Pty Ltd* (Privacy) [2026] AICmr 41 (11 June 2026); *Commissioner Initiated Investigation into Monash IVF Pty Ltd* (Privacy) [2026] AICmr 40 (11 June 2026); *Privacy Act Review Report* (February 2023) 94 <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>.

[11] Attorney-General's Department, *Privacy Act Review Report* (February 2023) 12 (Proposal 20.2) <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>.

[12] *Digital ID Act 2024* (Cth) s 55.
[13] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation) art 17; *Data Protection Act 2018* (UK) s 47; *California Consumer Privacy Act 2018,* Cal. Civ. Code § 1798.100 et seq, s 1798.130.
[14] Attorney-General's Department, *Privacy Act Review Report* (February 2023) 174 <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>; Lucinda Thorpe, 'Your Data, Their Rules: Australians Need Data Deletion Rights' *Digital Rights Warch* (Blog Post) 16 October 2025 <https://digitalrightswatch.org.au/2025/10/16/your-data-their-rules-australians-need-data-deletion-rights/>.
[15] Commonwealth, *Parliamentary Debates*, House of Representatives, 24 June 2009, 6989 (Craig Anthony Emerson, Minister for Small Business) <https://parlinfo.aph.gov.au/parlInfo/download/chamber/hansardr/2009-06-24/toc_pdf/69153.pdf;fileType=application%2Fpdf#search=%22chamber/hansardr/2009-06-24/0078%22>.
[16] See, e.g., Daniela Pizzirani and Dannielle Maguire, 'Facial recognition technology 'scope creep' is upon us, experts warn' *ABC News* (Online, 1 September 2026) <https://www.abc.net.au/news/2026-09-01/supermarket-violence-retail-crime-facial-recognition-technology/107056936>; Ima Caldwell, 'WA police facial recognition trial launches with a real-time arrest – and backlash over privacy' *The Guardian* (Online, 20 July 2026) <https://www.theguardian.com/australia-news/2026/jul/20/western-australia-police-real-time-facial-recognition-trial-privacy-ntwnfb>.
[17] Josh Taylor, 'Pay with a glance at a screen as biometric technology company begins push into Australian retail' *The Guardian* (online, 13 August 2026) <https://www.theguardian.com/australia-news/2026/aug/13/pay-with-a-glance-at-a-screen-as-biometric-technology-company-begins-push-into-australian-retail>.
[18] Daniela Pizzirani and Dannielle Maguire 'Coles and Woolworths Test Facial Recognition Technology' *ABC News* (online, 17 August 2026) <https://www.abc.net.au/news/2026-08-17/coles-and-woolworths-to-test-facial-recognition-technology/107045036>.
[19] See, e.g., Josh Taylor, 'Kmart sells out of low-cost rival to Meta camera glasses across Australia amid warnings of 'privacy nightmare' *The Guardian* (Online) 4 August 2026 <https://www.theguardian.com/australia-news/2026/aug/04/kmart-camera-glasses-anko-meta-smartglasses-australia>.
[20] Meta, How to live-stream to Facebook or Instagram on Ray-Ban Meta (Gen 1) glasses', *Meta AI glasses help centre* (web page, April 2026) <https://www.meta.com/en-gb/help/ai-glasses/1384089832459749/?srsltid=AfmBOorXGucBna5eOTCzwjSffWudJmYQ-r-N_H-RQMUpMZLiw181Jgtl> Dhruv Mehrotra and Dell Cameron, 'Meta Silently Added Face-Recognition Code for Its Smart Glasses to Millions of Phones' *WIRED* (online, 4 June 2026) <https://www.wired.com/story/meta-smart-glasses-face-recognition-nametag-connections/>
[21] HTI's model law was positively referred to in: Attorney-General's Department, *Privacy Act Review Report* (February 2023) 126 –127.
[22] Australian Government, *Government Response to the Privacy Act Review Report* (Report, 28 September 2023), 6 <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>; Proposal 6.2 in Attorney-General's Department, *Privacy Act Review Report* (February 2023) <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>.
[23] Australian Government, *Government Response to the Privacy Act Review Report* (Report, 28 September 2023), 28 <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>; Proposal 13.1 in Attorney-General's Department, *Privacy Act Review Report* (February 2023) <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>.
[24] eSafety Commissioner, *Smart glasses and online safety: When the camera disappears* (August 2026) <https://www.esafety.gov.au/industry/tech-trends-and-challenges/convergence-series/smart-glasses-and-online-safety>.
[25] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation) art 82; *Privacy Act 2020* (NZ) s 98
[26] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey* (May 2026) 26 <https://www.oaic.gov.au/__data/assets/pdf_file/0023/264362/ACAPS-2026-Report.PDF>.
[27] *Privacy Act 1988* (Cth) s7B(3).
[28] Human Technology Institute, *Surveillance Creep: Tech-enabled Surveillance of Australian workers* (March 2026) <https://www.uts.edu.au/news/2026/03/australian-law-must-protect-workers-from-harmful-tech-enabled-surveillance/contentassets/hti-snapshot-report-worker-surveillance.pdf>.
[29] Australian Law Reform Commission, *For your information: Australian privacy law and practice* (ALRC Report 108, August 2010) [33.44].
[30] Attorney-General's Department, *Portfolio Budget Statements 2026-27: Office of the Australian Information Commissioner – Entity resources and planned performance* (June 2026) 4 <https://www.ag.gov.au/system/files/2026-05/2026-27-ag-pbs-oaic.PDF> IDM, 'Funding Squeeze hits

OAIC as Privacy Reforms Land' *Blog Post* (15 May 2026) <https://idm.net.au/article/0015590-funding-squeeze-hits-oaic-privacy-reforms-land>.

[31] Office of the Australian Information Commission, *Corporate plan 2026-27* (August 2026) <https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/corporate-plans/corporate-plan-202627#section-overview>.