Zen Dodd
POLICY AND PUBLIC SUBMISSIONS

06 SEP 2026

Submission on the Privacy Reform Exposure Draft and Consultation Paper

Attorney-General's Department - Australia

steadytao.com/s/69ee429c

Executive Summary

I broadly support the Privacy Amendment (Personal Data Protection) Bill 2026. The updated definitions, consent requirements, APP 11 reforms, breach-response duties, processor framework and right to erasure would improve the Privacy Act.

My main concern is proposed APP 3. Existing collection and secondary-use limits would become factors within a holistic fair and reasonable test. The final Bill should retain a minimum requirement that collection be reasonably necessary and proportionate to a legitimate purpose. A materially incompatible later use should require consent, authority under Australian law, a court or tribunal order or a permitted general or health situation.

Proposed APP 4.3(b) should also be narrowed. Sensitive information does not lose its character merely because it appears in a public document or social-media post. The requested-service exceptions should use the necessity language described in the consultation paper and information collected under the strict-necessity exception should remain limited to providing that service.

The right to erasure should apply to all APP entities, with staged commencement where implementation capacity requires it. The Bill should preserve APP 1 and APP 11 when the human-research exception applies and require controller instructions to address the practical work needed to fulfil privacy rights through processors. The proposed geolocation definition should protect a precise location without first requiring tracking over time. Wearable systems also need safeguards for bystanders who cannot meaningfully consent.

1. Introduction

I make this submission in my personal capacity. The views are my own and should not be attributed to any organisation, project or other party with which I am associated. I work in cyber security and open-source software so I am mainly interested in how the proposed rights and obligations will work once they become databases, retention jobs, access controls, vendor instructions, breach procedures and account settings.

The reforms should proceed but several provisions need clearer minimum rules. An entity should be able to explain why it holds personal information, where the information is located, which suppliers handle it and how a person can exercise their rights without providing excessive new identification.

2. Fair and reasonable handling

The Bill would replace the current framework in APPs 3, 4 and 6. Proposed APP 3 would prohibit collection, use or disclosure unless it is fair and reasonable in the circumstances and lawful. The entity must consider reasonable expectations, its functions or activities, transparency, data minimisation, genuine choice, privacy impact, risk of harm, proportionality against benefits and the best interests of a child where relevant.[1]

I support a fair and reasonable test that applies throughout the information lifecycle. The concern is that no factor controls the result. The consultation paper says that collection necessity and purpose limitation would no longer operate as standalone requirements. It also says there would be no express consent requirement for an unexpected or unrelated secondary use.[1]

The OAIC's 2020 Privacy Act Review submission took a similar mixed approach. It supported scalable principles and also recommended binding rules where particular risks require greater certainty.[2]

The final Bill should retain two minimum limits beneath the broader test.

First, collection should be reasonably necessary and proportionate to a legitimate and specific purpose. If an entity can reasonably provide the relevant function using materially less personal information or information that is not personal, it should do so. Transparency, security and commercial benefit should not rescue unnecessary collection.

Second, a later use or disclosure that is materially incompatible with the original purpose should require a defined basis. That basis could be the individual's consent, authority under Australian law or a court or tribunal order, a permitted general or health situation or another express exception in the Act. Necessary administration, security and fraud prevention can

be handled through those defined routes without giving every broadly described corporate activity the same weight as the purpose for which the individual supplied the information.

The Department should publish a non-regression comparison before the Bill is introduced. It should take representative conduct currently governed by APPs 3, 4 and 6 and explain whether the proposed APP 3 changes the result. That would expose any accidental loss of protection and give regulated entities more useful guidance than abstract statements about the factors.

3. Sensitive information and requested services

Proposed APP 4.3(b) removes the usual consent requirement where sensitive information is collected from a publicly available document. That definition includes documents available after an ordinary person pays, registers or creates an account. The consultation paper says it may include social-media posts.[3]

This exception is too broad. A person may discuss their health, religion, sexuality or politics in public for reasons that have nothing to do with commercial profiling. Another person may also publish sensitive information without their permission. The fair and reasonable test still applies but public availability should not remove the consent requirement by itself.

The exception should be limited to information the individual has clearly made public themselves where the new collection remains reasonably connected to that context. Separate exceptions can cover Australian law, legal proceedings, public-interest activity and the permitted general and health situations. Large-scale scraping, enrichment, trading and consequential profiling should not receive a sensitive-information consent exception merely because the source was accessible.

The OAIC has previously identified collection from public websites and the dark web where information appeared to have been obtained unfairly, unlawfully or through a data breach. It recommended requiring entities collecting from third parties to take reasonable steps to satisfy themselves that the original collection complied with APP 3.[4] A proportionate provenance check should form part of any public-document exception.

Two requested-service provisions should also be aligned with the consultation paper. Proposed section 6FC(2)(a) excludes a disclosure from the definition of trade when it is "for the purposes of" the recipient providing a requested service. The consultation paper instead describes disclosure that is necessary to provide that service.[5] The operative provision should use the narrower necessity test.

Proposed APP 4.4 permits collection of sensitive information without consent when it is strictly necessary to provide a requested good or service. The consultation paper says that information collected through this exception may only be used or disclosed to provide the requested service.[6] That continuing purpose limit should appear in the legislation rather than guidance alone.

4. Erasure, processors, research and security

I support introducing APP 14 but the right should apply to all APP entities. A person would be able to initiate deletion and receive a written outcome rather than relying entirely on the entity's own APP 11 assessment.

The implementation must account for primary records, indexes, caches, derived profiles, processors and backups. A completed request should leave enough bounded evidence to prevent a restored backup or rebuilt index from silently returning deleted information to ordinary use. An entity relying on technical infeasibility should identify the affected information, document what it attempted, restrict ordinary use where possible and reassess the exception when its systems change.

Erasure requests also need proportionate identity checks. An attacker should not be able to delete another person's information but an entity should not demand identity documents where an existing authenticated account, previously established information or an authorised representative provides sufficient assurance. Any additional verification information should be limited to what is needed for the request and destroyed when it is no longer required.

Thirty days is a reasonable default for an APP 14 response, with a notified extension for a genuinely complex or unusually broad request. This is consistent with the existing Australian framework: OAIC guidance says an organisation's reasonable period for APP 12 access should generally not exceed 30 calendar days. The OAIC also currently tells complainants to allow an entity 30 days before escalating a privacy complaint.[7]

The same 30-day default should apply to internal privacy complaints. The consultation paper proposes 60 days, although the OAIC currently tells people that they may escalate a complaint if the entity has not responded within 30 days. A reasoned

extension may be appropriate for a genuinely complex matter but 60 days should not become the ordinary period before regulatory escalation is available.[7]

APP 14 should not depend on whether the holder belongs to a business group with at least $500 million in gross revenue, serves an average of 2.5 million monthly end users in Australia or operates a listed service. Those thresholds may justify staged commencement but they do not change the individual's privacy interest in information held about them.[8]

The Bill should establish the general right now, beginning with large digital platforms and extending it to other defined classes on a published timetable where immediate universal commencement is impractical. Proposed section 6EB(1) only permits prescription within the listed service types, so the current mechanism cannot later extend APP 14 across the rest of the economy.[8]

Schedule 6 would generally attribute a processor's compliant conduct to its controller while leaving processors directly responsible for APP 1 and APP 11. Proposed section 16D requires written instructions about the controller's purposes but does not set minimum operational content.[9] Controllers should be required to ensure that those instructions address access, correction and erasure assistance, incident cooperation, end-of-service return or deletion and equivalent obligations for sub-processors where relevant. A person should receive one coherent response from the controller rather than being sent between suppliers.

Texas HB 4 provides one practical comparator. Its processor duties cover assistance with rights requests, security and breach obligations, return or deletion after service, compliance evidence and equivalent contracts with subcontractors.[10]

Proposed section 94B is broader. It can prevent an act done in qualifying human research from breaching any APP. The final Bill should expressly preserve APP 1 and APP 11 or prevent the human research guidelines from displacing their baseline governance and security duties. The exception should not commence before the binding guidelines are in force.[11]

The APP 11 amendments should otherwise proceed. An entity cannot secure or destroy information reliably if it cannot identify what it holds. Regular evaluation should involve testing actual controls, deletion jobs, backup handling and de-identification rather than reviewing a policy document alone.[12]

The proposed breach-response duties should also proceed. The requirement to prepare for breaches, mitigate actual or suspected harm and notify the Commissioner within 72 hours after reaching the statutory belief threshold is practical. Guidance should distinguish detection, escalation, assessment and the point at which the entity had reasonable grounds to believe an eligible breach occurred. An incomplete initial statement is preferable to delaying notification until every fact is known.[13]

5. Emerging-technology questions

Question 1: Are the proposed updated definitions sufficient to address the risks of emerging technologies?

The revised definitions are a substantial improvement. Personal information can include generated information, behaviour, identifiers and information that allows a person to be singled out. The treatment of derived sensitive information also recognises that an inference can create risk even when the source data did not appear sensitive.[14]

The precise-geolocation definition remains too narrow because it requires information to be collected and held by reference to location over time. A single location can reveal that a person is at a refuge, medical clinic, protest, union meeting or religious service. Precise geolocation should be sensitive information without the temporal requirement. Repeated tracking should increase the assessed risk rather than determine whether protection begins.

Question 2: Is the definition of 'collection' sufficiently flexible to capture information collected via new technologies such as wearables?

It is mostly flexible enough to cover information generated or derived by wearables and AI systems. The continued connection to inclusion in a record or generally available publication may create uncertainty where a device transiently captures personal information, analyses it and acts on the result without retaining the original input.[15] The Department should clarify when transient capture, on-device analysis and retained inferences amount to collection and handling under the Act.

Question 3: To what extent can the reforms ensure that consent is meaningful, given that wearable technologies compromise the transparency of captures and uses of individuals' personal information?

The proposed requirement for consent to be voluntary, informed, current, specific and unambiguous would improve the position of device users.[16] Consent cannot carry the entire burden. Nearby people cannot realistically review terms whenever smart glasses, earbuds or connected vehicles capture them.

Regulated services should therefore minimise bystander collection, prefer on-device processing, use short default retention, avoid biometric identification and unrelated sensitive inference by default and prevent incidental captures from being traded or reused commercially. Recording indicators can improve awareness but do not create consent. Accessibility, journalism, emergency use and ordinary personal photography require careful boundaries; they should not be treated as equivalent to persistent commercial surveillance.

Question 4: Are existing remedial options adequate, including to ensure that individuals whose privacy has been interfered with can seek removal of relevant content? If not, what additional measures should be considered (without duplicating existing powers)?

The proposed APP 14 right helps only where a large digital platform holds the information and no exception applies. That boundary is too narrow for the reasons set out above. The statutory privacy tort addresses serious invasions but is not a routine correction or removal process.

Where a regulated entity controls stored content or a derived profile, people should have a clear route to request correction, removal or restricted use while a dispute is assessed. Immediate deletion may be inappropriate where the information must be preserved as evidence. In that case the entity should be able to place it beyond ordinary processing while retaining the minimum necessary for review. GDPR Article 18 provides an established example of restricted processing during disputes about accuracy, lawfulness or an objection.[17] Guidance should map these remedies against existing platform, privacy, defamation and online-safety processes so that new rules do not duplicate an available remedy.

Question 5: To what extent will the existing or proposed measures encourage improved compliance?

The APP 11 identification and ongoing-evaluation duties, together with the positive breach-response duties, should improve compliance because they require knowledge of actual systems and evidence that controls work. The effect will depend on guidance and enforcement.

The OAIC should publish practical examples for the implementation issues identified above before commencement. The Government should then measure response times, refusal grounds, repeated technical-infeasibility claims, notification timeliness and recurring control failures. Those measures should not require entities to collect additional sensitive information merely to report attractive statistics.

6. Recommendations

I recommend that the Department:

- preserve separate minimum requirements for necessary and proportionate collection and for materially incompatible secondary uses;
- narrow the publicly available document exception for sensitive information and require proportionate checks of source provenance;
- align section 6FC(2)(a) and APP 4.4 with the requested-service safeguards described in the consultation paper;
- use 30 days as the ordinary period for APP 14 requests and internal privacy complaints, with notified extensions for genuinely complex matters;
- preserve APP 1 and APP 11 under the human research exception and commence it only after the binding guidelines are in force;
- require controller instructions to cover the operational assistance needed to fulfil privacy rights through processors;

- remove the "over time" requirement from precise geolocation and address bystander information through design and purpose limits;
- retain the APP 11 and breach-response reforms, supported by practical implementation guidance; and
- establish APP 14 as a general right for all APP entities, with staged commencement where implementation capacity requires it.

7. Drafting corrections

The following points should be checked before the Bill is introduced.[18]

1. Schedule 4, item 7 refers to APP 14.4(c) but proposed APP 14.4 contains only paragraphs (a) and (b). The notice obligation appears in APP 14.4(b)(ii).
2. The notes to proposed APP 3.3 and APP 4.6 refer to paragraph 4.2(a) but APP 4.2 has no paragraph (a). The relevant collection exceptions appear in APP 4.3(a).
3. Proposed section 6FC(2)(a) uses "for the purposes of" where the consultation paper says the requested-service carve-out applies when disclosure is necessary to provide the requested product or service.
4. Proposed APP 4.4 contains the strict-necessity collection exception but does not state the consultation paper's further condition that the sensitive information may only be used or disclosed to provide the requested good or service.
5. Clause 2 leaves the commencement table blank. The consultation paper says the human research exception is intended to commence once the human research guidelines are in place so the final commencement provisions should make that dependency explicit.

References

[1] Attorney-General's Department, *Privacy Amendment (Personal Data Protection) Bill 2026: Exposure Draft*, Schedule 2, item 10, proposed APP 3.1-3.2; Attorney-General's Department, *Privacy Reform: Consultation Paper*, pp. 10-15.

[2] Office of the Australian Information Commissioner, *Privacy Act Review Issues Paper submission, Part 3: Flexibility of the APPs in regulating and protecting privacy*, 11 December 2020, paras 3.1-3.21.

[3] Attorney-General's Department, *Privacy Amendment (Personal Data Protection) Bill 2026: Exposure Draft*, Schedule 2, items 1 and 10, proposed APP 4.3(b); Attorney-General's Department, *Privacy Reform: Consultation Paper*, pp. 16-17.

[4] Office of the Australian Information Commissioner, *Privacy Act Review Issues Paper submission, Part 3: Flexibility of the APPs in regulating and protecting privacy*, paras 3.26-3.33.

[5] Attorney-General's Department, *Privacy Amendment (Personal Data Protection) Bill 2026: Exposure Draft*, Schedule 2, item 7, proposed s 6FC(2)(a); Attorney-General's Department, *Privacy Reform: Consultation Paper*, p. 16.

[6] Attorney-General's Department, *Privacy Amendment (Personal Data Protection) Bill 2026: Exposure Draft*, Schedule 2, item 10, proposed APP 4.4; Attorney-General's Department, *Privacy Reform: Consultation Paper*, p. 17.

[7] Office of the Australian Information Commissioner, *Chapter 12: APP 12 Access to personal information*, paras 12.66-12.67; Office of the Australian Information Commissioner, *Before you lodge a privacy complaint with us*, updated 2 March 2026; Attorney-General's Department, *Privacy Reform: Consultation Paper*, p. 38.

[8] Attorney-General's Department, *Privacy Amendment (Personal Data Protection) Bill 2026: Exposure Draft*, Schedule 4, item 6, proposed s 6EB(1), (2) and (8).

[9] Attorney-General's Department, *Privacy Amendment (Personal Data Protection) Bill 2026: Exposure Draft*, Schedule 6, items 2, 4 and 6, proposed ss 6A(2A), 6B(2A) and 16D.

[10] Texas Legislature, *HB 4: Texas Data Privacy and Security Act, enrolled text*, 2023, s 541.104.

[11] Attorney-General's Department, *Privacy Amendment (Personal Data Protection) Bill 2026: Exposure Draft*, Schedule 5, item 2, proposed s 94B; Attorney-General's Department, *Privacy Reform: Consultation Paper*, p. 36.

[12] Attorney-General's Department, *Privacy Amendment (Personal Data Protection) Bill 2026: Exposure Draft*, Schedule 3, item 22, proposed APP 11.4-11.5.

[13] Attorney-General's Department, *Privacy Amendment (Personal Data Protection) Bill 2026: Exposure Draft*, Schedule 3, items 7 and 10, proposed ss 26WDA-26WDB and 26WK; Attorney-General's Department, *Privacy Reform: Consultation Paper*, pp. 23-28.

[14] Attorney-General's Department, *Privacy Amendment (Personal Data Protection) Bill 2026: Exposure Draft*, Schedule 1, items 6, 9 and 12, proposed ss 6AAA and 6FD-6FG; Attorney-General's Department, *Privacy Reform: Consultation Paper*, pp. 4-9.

[15] Attorney-General's Department, *Privacy Amendment (Personal Data Protection) Bill 2026: Exposure Draft*, Schedule 1, item 9, proposed s 6AAA.

[16] Attorney-General's Department, *Privacy Amendment (Personal Data Protection) Bill 2026: Exposure Draft*, Schedule 1, item 10, proposed s 6AAB; Attorney-General's Department, *Privacy Reform: Consultation Paper*, pp. 8-9.

[17] European Parliament and Council, *Regulation (EU) 2016/679 (General Data Protection Regulation)*, Article 18.

[18] Attorney-General's Department, *Privacy Amendment (Personal Data Protection) Bill 2026: Exposure Draft*, cl. 2, Schedule 2, items 7 and 10, Schedule 4, items 7 and 11 and Schedule 5, item 2; Attorney-General's Department, *Privacy Reform: Consultation Paper*, pp. 16-17 and 36.