

17 September 2026

To the Attorney-General's Department

By submission: [Attorney-General's Department – Consultation Page](#)

RE: Privacy Reform – Consultation on Exposure Draft legislation

The Internet Association of Australia Ltd (**IAA**) thanks the Attorney-General's Department (**Department**) for the opportunity to respond to the Consultation Paper and exposure draft *Privacy Amendment (Personal Data Protection) Bill 2026*.

IAA is a member-based association representing Australia's Internet community. Our membership is largely comprised of small to medium sized Internet service providers (**ISPs**) in the Australian telecommunications market. IAA have been actively engaged in the Government's privacy reform, having responded to the Department's past consultation on previous stages of reform to Australia's privacy framework. While many of our members would fall under the small business threshold of the *Privacy Act 1988 (Cth)* (**Privacy Act**), as telecommunications entities subject to the *Telecommunications (Interception and Access) Act 1979 (Cth)* (**TIA Act**), they still fall within the scope of the Privacy Act in relation to certain datasets and practices.

Moreover, as the telecommunications sector underpins the digital age, we are highly interested in and supportive of ensuring the legislative framework remains fit for purpose to support a thriving digital age, while also ensuring there are robust protections in place for individuals' data and privacy protection. Thus, from the outset, IAA emphasise our commitment, and that of our members, to the Government's objective to strengthen Australia's privacy framework to better strengthen modern data practices.

However, we also consider that effective privacy legislation must be practicable and encourage meaningful compliance. To that end, we raise concerns about the consultation process itself which we do not consider to be sufficient for a reform package of this size and significance. In order for the reformed privacy framework to achieve its intended outcomes, industry and other stakeholders must be afforded a genuine and adequate opportunity to understand, test and respond to the proposed changes.

As abovementioned, our members comprise smaller operators within the telecommunications industry who typically lack the resources and regulatory expertise to engage in regulatory reform processes, and yet are most disproportionately affected by the resulting regulatory burden. We also therefore make recommendations throughout our response to suggest practical ways Government can ensure the proposed reforms are implemented in a manner that is proportionate and workable in consideration of smaller industry participants, to help support its policy intent.

OUR RESPONSE

OVERARCHING COMMENTS

Consultation Approach

Prior to addressing the specific proposed reform, IAA and our members express our significant concerns in

relation to the compressed consultation period. The reforms proposed are substantial, including significant structural changes to widely understood existing practices surrounding collection with consent, as well as key definitional changes that would broaden the scope of what is considered ‘personal information’. The implications of these definitional and conceptual changes will be discussed further below.

We do not consider a consultation timeframe of less than one month to be sufficient for a law reform package of this scale and significance. Indeed, the Office of Impact Analysis’ best-practice guidelines recommends a minimum consultation period of 30 days, extending up to 60 days for proposals of greater significance.¹ We consider this longer period necessary given the scope and complexity of the proposed changes to the privacy framework.

Furthermore, we highlight that the short consultation timeframe disproportionately affects smaller entities, such as our members who lack dedicated in-house privacy counsel and regulatory personnel. These entities often already face difficulties engaging in regulatory reform processes, but the lack of adequate time and dedicated sector engagement compounds this disadvantage, which increases the risk that the resulting legislative framework will not be proportionate, and will impose greater regulatory burdens on smaller entities.

We are further concerned about the consultation approach itself, which has been limited to written submissions, with the Department not holding any town-hall sessions or similar forums. We reiterate the resource constraints of smaller entities where requiring written feedback in response to the Exposure Draft and Consultation Paper as the sole means of consultation is prohibitive to their meaningful engagement with the reform process.

Additionally, we raise that the Department has not conducted any dedicated sector-specific engagement to thoroughly tease out industry concerns, particularly given proposed reforms would intersect with existing, highly technical telecommunications-specific obligations. This is again inconsistent with consultation best practice. Especially as even small telecommunications entities who may otherwise fall under the ‘small business’ threshold are subject to certain privacy obligations in accordance with the TIA Act.

We therefore recommend the consultation period should be extended to at least 60 days to provide stakeholders with sufficient time to thoroughly consider and respond to the proposed changes.

Furthermore, during the extended consultation period, the Department should:

- **engage with stakeholders through town-halls or other similar forums, to provide alternative avenues for stakeholders to provide feedback;**
- **conduct sector-specific consultation on matters that would intersect with existing sector-specific regulation.**

Implementation Approach

We understand that the Department has yet to determine the commencement timeframe for the proposed changes. Reiterating the significant nature of the reform, it is imperative that entities are afforded a reasonable opportunity to understand and implement the changes necessary to not only ensure compliance, but to ensure genuinely improved privacy conditions. Furthermore, in recognition of the smaller entities that are resource constrained and require greater assistance to navigate regulatory reform, we consider a longer implementation timeframe is required, during which period, the Department and OAIC should actively engage with these entities to ensure thorough awareness and understanding of the changes.

¹ <https://oia.pmc.gov.au/sites/default/files/2023-08/best-practice-consultation.pdf>

The commencement timeframe to be specified under section 2 of the Exposure Draft should be reasonably set to provide staged implementation timeframes as necessary for the various aspects of implementation.

SCHEDULE 1 – CORE DEFINITIONS

‘Personal information’ and ‘reasonably identifiable’

We reiterate that amendment of this core term, ‘personal information’ is a significant change to the foundation of the Privacy Act, and requires sufficient time for stakeholders to properly understand, consider and respond to its implications.

In particular, the broadened coverage to include information that ‘relates to’ an individual, in addition to the context-dependent identifiability test in the amended definition, would require ongoing legal judgement calls that smaller telecommunications entities lack the in-house expertise to make.

We recommend explicit OAIC guidance material to be developed specifically for the telecommunications context. In particular, we seek guidance illustrating how the ‘relates to’ and ‘reasonably identifiable’ tests apply to common telecommunications data categories such as network performance, faults and coverage data, including practical examples as to when such data would and would not be treated as ‘personal information’.

Additionally, we request this clarity should be provided prior to the commencement of the amended definitions so that entities are provided with genuine and reasonable opportunity to review and adjust their data-handling practices accordingly.

Precise geolocation tracking data

Similarly, the explicit classification of ‘precise geolocation tracking data’ as ‘sensitive information’ has significant ramifications for telecommunications entities as it interacts with various privacy obligations and the TIA Act. We consider this will cause smaller entities considerable confusion and anxiety as to how these obligations and corresponding exceptions (such as proposed APP 4.3) apply in different scenarios. This is particularly the case for mobile virtual network operators (MVNOs) and resellers that do not control the underlying network infrastructure generating location data, which would raise further questions as to which entity bears responsibility for collection, consent, retention and access obligations.

We therefore recommend that the Department, in consultation with the OAIC and Department of Home Affairs, provide comprehensive and plain-English guidance to address the interaction between the Privacy Act and TIA Act in relation to metadata that would constitute ‘sensitive information’.

Consent

Again, we consider the changes to ‘consent’ processes as a substantive structural amendment that underpins existing and established operational processes. This is particularly the case given the resulting complexity of where consent would be required under the proposed framework: in relation to sensitive information, consent is required unless an exception applies, whereas in relation to non-sensitive personal information, no consent is required and collection is justified, so long as it is fair and reasonable.

The complexity is further compounded by the Department’s view that bundled consent is unlikely to satisfy the ‘voluntary’ and ‘specific’ limbs of the amended consent definition. In practice, a single customer interaction, such as during sign up, will typically involve the collection of multiple categories of personal information, only some of which requires consent.

This new framework is therefore likely to cause significant confusion for smaller telecommunications entities. Again, we reiterate the resource constraints of smaller entities who are typically unable to navigate

this level of regulatory complexity.

We recommend the development of comprehensive guidance that assists telecommunications entities to navigate the complex consent obligations. In particular, we request a telecommunications-specific workflow or decision tree diagram that explicitly distinguishes:

- where collection of personal information or sensitive information is legally required (and therefore, consent is not required);
- where implied consent would be reasonably taken to have been provided; and
- where express, unbundled consent would be required.

SCHEDULE 2 – HANDLING PERSONAL INFORMATION

Fair and Reasonable test

As discussed above in relation to the proposed amendments to ‘consent’, we consider the proposed introduction of a ‘fair and reasonable test’ to replace the existing consent process for collection, use and disclosure of personal information represents a substantial departure from an established and well-understood compliance framework. While we support and appreciate that not each legislated factor will need to be satisfied in order to meet the ‘fair and reasonable’ test, we are concerned that this will cause significant uncertainty as to what is required in practice.

We reiterate our recommendations above for the development of extensive, sector-specific guidance that addresses telecommunications data-handling practices and scenarios.

Consent to trade personal information

We also request clarification on how the proposed change would affect entities who purchase and therefore collect and use personal information, such as lead-generation data. We understand that under APP 4.2, the obligation to acquire consent for the collection, use and disclosure of personal information for the purposes of trade would fall on the disclosing entity selling the personal information (**broker**). However, the fair and reasonable test under APP 3 suggests that purchasing entities who then use such information must independently satisfy the fair and reasonable test, having regard to factors such as the individual’s reasonable expectations, and the transparency of the original collection.

In practice, the purchasing would have limited visibility into the broker’s collection practices, and no means to verify whether the broker validly obtained consent for the original collection and subsequent trade and use of the personal information. This creates a risk for purchasing entities who could be held liable for breaching the fair and reasonable test, despite having played no part in the original collection and consent practices.

We therefore recommend clear safe harbour principles for entities that purchase personal information from a third party to demonstrate reasonable compliance with the fair and reasonable test where it obtains warranties from the broker in relation to its consent and collection practices.

Notification of collection

IAA takes this opportunity to request practical OAIC guidance and assistance with industry’s compliance efforts – particularly for smaller entities that have limited resources. For example, we note that the New Zealand counterpart to the OAIC – the Office of the Privacy Commissioner (New Zealand) maintains a Privacy Statement Generator to assist entities establish and maintain a compliant privacy statement.²

² <https://www.privacy.org.nz/responsibilities/privacy-statement-generator/>

We recommend that the OAIC develops similar tools in respect of privacy collection notifications, and other statements or documentation that an entity is obliged to establish and provide to provide practical assistance to entities subject to the Privacy Act.

Part 2 - Permitted General Situation

As above, we request explicit guidance with sector-specific examples of how the permitted general situation exceptions would apply in the telecommunications context.

SCHEDULE 3 – DATA SECURITY

Part 1 - Notifiable Data Breach

IAA supports the amendments to the notifiable data breach regime in principle. However, we stress the importance of ensuring sufficient Government and OAIC support to ensure effective and meaningful compliance with data security obligations.

We reiterate the increasingly complex regulatory landscape for the telecommunications industry wherein entities face multiple notification obligations under various laws in the event of a data breach incident particularly where the breach involves a cyber security incident, including but not limited to the *Security of Critical Infrastructure Act 2018*, and *Cyber Security Act 2024*.

We recommend that the Department collaborate with the Department of Home Affairs, the OAIC and other relevant agencies to fast-track the development of a single notification portal that can be used by entities to satisfy the notification obligations under various laws where an entity is subject to a cyber security related data breach.

Part 2 - Security of Personal Info

We support in principle, the policy intent to improve data minimisation and security. However, we reiterate the difficulty for industry to navigate the complex regulatory landscape wherein entities must comply with various data retention requirements, each with different retention periods. This is further complicated by EDR schemes that effectively necessitate longer record keeping requirements due to complaints being able to be raised up to 6 years after service provision such as under the Telecommunications Industry Ombudsman scheme, in addition to varying limitation periods for litigation which drive entities to retain data longer than ‘reasonable’ expectations may anticipate.

We understand that the Department, in collaboration with the Department of Home Affairs has been conducting a Commonwealth data retention review with the aim to simplify and streamline data retention obligations and reduce compliance burdens for industry, and therefore also reduce privacy and cyber security risks. We consider it crucial that prior to the finalisation of the proposed reforms to the Privacy Act, Government also clarifies and simplifies existing data retention obligations. Importantly, as was noted in our response to the data retention review, the scope of the review did not extend to state or territory legislation, external dispute resolution schemes, or statutory limitation periods for litigation. As such, it is also appropriate that where Government seeks to tighten privacy obligations around minimisation and destruction, it also considers the cumulative effect of these other retention drivers.

SCHEDULE 4 – DATA ACCESS AND ERASURE

In principle, we support the proposed amendments and appreciate the proposed introduction of an exception to access request where technical constraints exist. However, we are concerned about the interpretation of ‘reasonable steps’ which may require entities to develop new and/or costly systems or otherwise undertake significant re-engineering of systems to satisfy this requirement. This would particularly disproportionately affect smaller telecommunications entities operating legacy or vendor-supplied systems who may have limited ability to control how access is provided. We appreciate that this concern must be

appropriately balanced against the risk of entities deliberately engineering complex technical systems to avoid providing access.

We therefore recommend clarification that ‘reasonable steps’ should not require an entity to build new systems or undertake substantial re-engineering of existing systems, particularly where the cost of doing so would be disproportionate to the entity’s size and resources.

Moreover, we also recommend the development of guidance identifying a non-exhaustive list of factors relevant to assessing ‘reasonable steps’ in this context.

OAIC POWERS AND EFFICIENCY

In principle, we support the proposed measures to ensure the OAIC has sufficient powers to ensure effective enforcement of the Privacy Act. However, given these changes are substantial and reiterating the limited resources of smaller entities to track and understand regulatory reform, we request commitment to a collaborative and educative enforcement approach, prior to pursuing enforcement action against non-compliance with complaint handling obligations, unless such breaches demonstrate serious negligence or wilful non-compliance.

Furthermore, we are concerned about the scope of the reasonable assistance powers, particularly where it may affect smaller telecommunication entities by subjecting resource constrained entities to provide onerous technical assistance. We consider further scoping is required to set parameters around what is considered reasonable assistance and to ensure appropriate safeguards exist.

ADDRESSING EMERGING TECHNOLOGIES

As ISPs are merely data conduits, we understand these entities are unlikely to be the intended entities to be subject to the proposed privacy protections in relation to smart glasses and other emerging AI technologies. **To that end, we consider it crucial that any reform in relation to emerging technologies sufficiently makes clear that telecommunications entities are not held inadvertently held responsible for data collection, protection or handling practices, simply by virtue of their role as data conduits.**

CONCLUSION

Once again, IAA appreciates the opportunity to contribute to the exposure draft and accompanying consultation paper on privacy reform. We reiterate our commitment to working with Government in its effort to strengthen Australia’s privacy framework and provide greater protections to individuals in the rapidly changing digital age. To that end, to support industry in the adoption of privacy best practices and meaningfully comply with any new privacy obligations, we recommend the Government to engage further with stakeholders, including through sector-specific consultations. We also urge the Department to recognise the unique position of smaller telecommunications providers who face major compliance burdens, and provide targeted support such as via appropriate transition timeframes, and a collaborative and educative approach as the changes are implemented. IAA looks forward to continue engaging with the Department, Government, industry and other stakeholders in the continued development of a privacy framework that will better serve Australia in the modern age.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia Ltd (**IAA**) is a not-for-profit member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (**WAIA**), the Association changed its name in early 2016 to better reflect our national membership and growth.

Our members comprise industry professionals, corporations, and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IAA regularly engages with government and regulatory bodies on policy matters affecting the Internet industry. In particular, our advocacy efforts represent the small to medium sized internet service providers in Australia who are often disproportionately disadvantaged by law reform affecting the telecommunications sector. Our public policy work is guided by the following principles:

We stand for an internet for the common good

We stand for an open internet platform

We stand for measured, effective and practical regulation

IAA is also a licenced telecommunications carrier and provides the IX-Australia service to Corporate and Affiliate members on a not-for-profit basis. It is the longest running carrier neutral Internet Exchange in Australia. Spanning seven states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.