Australian Telecommunications Alliance

Setting The Standard.
Driving Progress.

AUSTRALIAN TELECOMMUNICATIONS ALLIANCE SUBMISSION

To: Attorney-General's Department

Re: Exposure Draft of the *Privacy Amendment (Personal Data Protection) Bill 2026*

18 September 2026



CONTENTS

1. AUSTRALIAN TELECOMMUNICATIONS ALLIANCE 3

2. INTRODUCTION 3

3. REGULATORY COHERENCE AND HIERARCHY OF OBLIGATIONS 3

4. IMPACTS OF AN EXPANDED DEFINITION OF PERSONAL INFORMATION 4

5. FAIR AND REASONABLE TEST 5

6. ACCESS, ERASURE, RETENTION, AND PERMITTED USE CASES 6

7. PRECISE GEO-LOCATION DATA AND SENSITIVE INFORMATION 7

8. DATA CONTROLLERS AND PROCESSORS 8

9. DATA BREACH NOTIFICATIONS 9

10. MITIGATION OF HARMS 10

11. IMPLEMENTATION LEAD TIME AND REGULATORY GUIDANCE 11

1. AUSTRALIAN TELECOMMUNICATIONS ALLIANCE

1.1 The Australian Telecommunications Alliance (ATA) is the peak body of the Australian telecommunications industry. We are the trusted voice at the intersection of industry, government, regulators, and consumers. Through collaboration and leadership, we shape initiatives that grow the Australian telecommunications industry, enhance connectivity for all Australians, and foster the highest standards of business behaviour. For more details, visit www.austelco.org.au.

1.2 For questions on this submission, please contact Deputy CEO Christiane Gillespie-Jones, c.gillespiejones@austelco.org.au.

2. INTRODUCTION

2.1 The ATA welcomes the opportunity to provide a submission to the Attorney-General's Department on the exposure draft of the *Privacy Amendment (Personal Data Protection) Bill 2026* (Bill) and the associated consultation paper.

2.2 The telecommunications sector supports the objective of strengthening privacy protections. However, the effectiveness of those protections will depend on whether the new requirements can operate coherently with the sector's existing obligations (including as providers of essential communications services and critical infrastructure) and with the practical operation of services, devices, and digital products.

2.3 Telecommunications networks, connected devices, and associated digital services necessarily generate and use substantial volumes of technical, network, usage, location, and operational information. Much of this information is created to connect customers, route communications, operate device or product functionality, maintain and secure networks and products, investigate faults and fraud, respond to incidents, and meet statutory obligations. Privacy settings that do not take those functions into account may create compliance friction without producing a commensurate privacy benefit.

2.4 The ATA therefore encourages an implementation approach focused on operational certainty and consumer outcomes. The reforms should be supported by targeted drafting changes, workable exceptions, clear interaction rules, and practical, sector-specific guidance, rather than requiring entities to resolve uncertainty through defensive compliance practices.

2.5 The ATA also notes that the consultation period has materially constrained the time available for members to assess the Bill across complex systems and overlapping regulatory regimes. This submission accordingly focuses on the issues that members have been able to identify, at a high level, as most significant. The absence of comment on any other provision should not be taken as indicating support for that provision or an absence of concern. Despite a focus on key issues, the suggested 1,000-word limit is, unfortunately, unmanageable.

3. REGULATORY COHERENCE AND HIERARCHY OF OBLIGATIONS

3.1 A central issue for the telecommunications sector is the interaction between the proposed privacy reforms and the extensive existing framework governing telecommunications, cyber security, critical infrastructure, data retention, law-enforcement access, consumer protection, complaints, and public safety.

3.2 The same information may be subject to different statutory or regulatory expectations concerning its collection, retention, deletion, security, disclosure, and reporting. Those expectations may arise under

telecommunications data-retention and interception or access requirements, complaint-handling and regulatory processes, court proceedings and statutory limitation periods, as well as cyber-security and critical-infrastructure obligations, and spam or scam-related obligations. For example, it is unclear how compliance with a request for deletion of personal information interacts with a customer's right to initiate a complaint with the Telecommunications Industry Ombudsman and the need for the existence of the (deleted) data to respond to the complaint. (Also refer to section 6.)

3.3 The issue is particularly acute during a live security or service incident. A provider may simultaneously need to preserve evidence, contain a threat, maintain essential services, respond to regulators and law-enforcement agencies and emergency services providers, and communicate with customers. Directions or expectations from different authorities may not always align in timing, content, or operational effect.

3.4 For example, connected devices and associated digital services may be subject to overlapping privacy, online safety and children's privacy requirements concerning the same data-handling activities, including data minimisation, age assurance, consent, and retention.

3.5 The proposed broader concept of personal information will magnify this interaction by bringing a larger range of technical and operational data within the privacy framework. In the absence of clear interaction rules, organisations may retain personal information defensively because the circumstances in which deletion is permitted or required by other frameworks are uncertain.

3.6 Uncertainty about which obligation prevails creates legal and operational risk and can divert resources from the substantive objective of protecting customers. Regulated entities should not be placed in breach of one regime because they have complied, reasonably and in good faith, with another applicable statutory duty or lawful regulatory direction.

3.7 The framework should therefore make clear how Privacy Act obligations interact with other Commonwealth, state and territory requirements, including where duties overlap or point to different operational outcomes. Coordination between regulators will be particularly important during fast-moving incidents.

Recommendation 1

Establish a clear interaction framework between Privacy Act obligations and other statutory and regulatory requirements.

Where duties conflict or overlap, the legislation or authoritative guidance should identify priority rules, facilitate regulatory coordination, and provide an appropriate safe harbour for entities acting reasonably and in good faith to comply with another applicable legal obligation or lawful direction.

4. IMPACTS OF AN EXPANDED DEFINITION OF PERSONAL INFORMATION

4.1 The ATA recognises that the proposed change from information 'about' an individual to information that 'relates to' an individual is a central element of the reform package. The principal concern for our sector is the breadth and contextual uncertainty of the practical application of this shift.

4.2 Alternatively speaking, an expanded definition of personal information risks bringing into scope – and therefore creating significant additional regulatory burden and cost – data types (such as technical, logging, and operational data) without necessarily providing tangible individual benefit, particularly when taking into consideration any appropriately scoped exemptions to access and erasure of such data.

4.3 Telecommunications and connected-device environments contain very large volumes of network, service, usage, device, premises, assurance, maintenance, diagnostic, and fault-management data. Depending on

context and the availability of other information, data that has traditionally been treated as technical, product-related, or operational may fall within the expanded definition.

4.4 Because the proposed test is contextual, the same data element may be personal information in one system or use case but not in another. This creates material challenges for consistent data classification and for identifying where personal information is held across complex and highly distributed environments.

4.5 A broader definition has consequential effects across the entire privacy lifecycle, including security controls, access and erasure processes, retention schedules, breach assessment, customer-service processes, and internal governance.

4.6 The ATA is also concerned that the proposed APP 11 obligation to identify personal information, when combined with the broader definition, may in practice be interpreted as requiring a comprehensive personal-information inventory across every system and data store.

4.7 An exhaustive inventory would be difficult to maintain in large, dynamic network environments and may impose substantial compliance effort without a proportionate benefit to individuals. A risk-based obligation to take reasonable steps to understand and govern the personal information held would be more workable and more likely to remain accurate over time.

4.8 Practical guidance should address telecommunications examples such as outage and fault information, premises connection records, service addresses, device identifiers and diagnostics, product telemetry, operational metadata, network-management records, maintenance and assurance data, and customer-service records.

Recommendation 2

If the broader definition is retained, accompany it with comprehensive and authoritative guidance, including telecommunications-specific examples and case studies.

Clarify that APP 11 requires reasonable and proportionate identification and governance of personal information, rather than an exhaustive inventory of every data element that could, in some context, relate to an individual.

5. FAIR AND REASONABLE TEST

5.1 The ATA supports the objective that the collection, use, and disclosure of personal information should be fair and reasonable. The proposed test is, however, highly contextual and may be difficult to operationalise consistently across large and complex telecommunications environments without more detailed guidance.

5.2 Our members require clarity as to how the test applies to ordinary activities such as outage management, connection management, network operation, device and product operation, maintenance, service and product improvement, fraud prevention, and incident response. These activities may not always be visible to customers but are integral to safe and reliable service and product delivery.

5.3 Safety and security should be expressly recognised as relevant considerations for the fair and reasonable test. Personal information may need to be used to protect customers, workers, and other persons, and to prevent, detect, investigate, respond to, and recover from cyber threats and incidents. A fair and reasonable assessment should be capable of recognising those legitimate objectives alongside the privacy impact.

5.4 The concept of 'genuine choice' also requires careful treatment. Some secondary uses are not optional features from our members' perspective but are important to the operation, maintenance, and improvement of networks, connected devices, and associated digital services for the broader customer base and the public. The test should not treat the absence of an individual opt-out as determinative where the use is

proportionate and supports a legitimate operational or public-interest purpose.

5.5 The child-related factors raise a particular issue for carriage service providers, device manufacturers, and equipment suppliers. Telecommunications services and connected devices are commonly acquired by an adult account holder or purchaser and subsequently used by a child. Providers, manufacturers, and suppliers generally do not know the age of the end user and should not inadvertently be required to introduce age-assurance processes merely in order to apply the fair and reasonable test.

5.6 Similarly, it may be difficult to assess what is in the best interests of a child where the organisation does not know that the information in question relates to a child. The framework should recognise this practical limitation and provide clear expectations for entities that do not ordinarily verify the age of service users.

5.7 The ATA is also concerned by the use of different thresholds such as 'necessary' and 'strictly necessary' in proposed APP 4.4. 'Reasonably necessary' is a familiar Privacy Act concept that already accommodates proportionality and data minimisation. Introducing a higher threshold without a clearly articulated policy reason risks uncertainty and inconsistent application.

Recommendation 3

Use a consistent 'reasonably necessary' threshold in APP 4.4 and related exceptions, rather than introducing a separate 'strictly necessary' standard unless a compelling policy distinction is clearly articulated.

Expressly recognise safety, cyber security, fraud prevention, resilience, service and product continuity, and network and device integrity as relevant considerations in the fair and reasonable assessment.

Clarify that the reforms do not of themselves require telecommunications providers, device manufacturers or equipment suppliers to undertake age assurance where they do not otherwise know the age of the service or product user.

6. ACCESS, ERASURE, RETENTION, AND PERMITTED USE CASES

6.1 The proposed reforms include large telecommunications providers in the definition for 'large digital platform' (via reference to the definition of 'relevant electronic service' in the *Online safety Act 2021*). The breadth of the definition may also capture online services provided by device manufacturers, and equipment suppliers. The ATA seeks clarity as to whether telecommunications providers, device manufacturers, equipment suppliers, and their individual services are intended to fall within the proposed concept of a 'large digital platform' for the purposes of the new erasure rights and access rights to information that may previously not have been in scope of the definition of personal information.

6.2 The definition of a 'large digital platform' captures a wide range of online services. Many global manufacturers and equipment suppliers will likely exceed the gross revenue threshold when considered on a group basis. If revenue is a factor that will be considered, it should only be applied on an individual service basis and to local (Australian) revenue for that service, rather than a group basis. This is necessary and reasonable to ensure there is no disproportionate impact.

6.3 If ATA members are intended to be captured, the associated rights must contain sufficiently broad and practical exceptions. A test based only on technical impossibility or infeasibility is too narrow: in modern systems, many actions are technically possible if enough time and cost are applied, even where the result would be disproportionate, unreasonable, or operationally impracticable.

6.4 Members may have legitimate reasons to retain information even where continued retention is not solely for the immediate benefit of the individual concerned or required under law. Those reasons include network operation and maintenance, service and network improvement, complaint investigation, future customer issues, regulatory investigations, litigation and legal defence, statutory limitation periods, cyber security, and fraud prevention.

6.5 Access and erasure should also be treated as distinct rights with distinct exceptions. There will be circumstances in which information may legitimately need to be retained but cannot lawfully or appropriately be disclosed, including because disclosure could prejudice security, investigations, legal obligations, or the rights of other persons.

6.6 These purposes can have a broader public and consumer benefit. Network performance and fault information, for example, may be needed to identify systemic issues and improve service reliability across the customer base even where the use is not directed to the individual from whom the data originated.

6.7 The ATA supports the policy objective of preventing the trading of personal information without appropriate consent. The exceptions must, however, be framed so that they do not impede legitimate fraud detection and prevention activities.

6.8 However, the proposed carve outs from the definition of trade should contemplate routine business-to-business data synchronisation, derived telemetry, and automated AI inferences. Without workable processor safe harbours exempting intermediary technology infrastructure, the operation of these rules in their broadened scope under its new definition of trading risk disruption of standard digital operations.

6.9 Members are also concerned that a fraud and scam-prevention exception would be too narrow if it depended on a pre-existing suspicion and disclosure by the recipient. Effective fraud and scam controls frequently rely on proactive detection, pattern analysis, and information sharing before a specific suspicion has crystallised.

6.10 The framework should accommodate activities that are reasonably necessary to prevent, detect, investigate, and remedy unlawful activity, or serious fraud and scam-related misconduct. A carefully bounded public-interest exception, supported by factors that entities must consider, may also be appropriate where the activity is proportionate and cannot sensibly depend on consent.

Recommendation 4

Clarify whether telecommunications providers, device manufacturers, equipment suppliers and their individual services are intended to be captured as large digital platforms. If they are, broaden the access and erasure exceptions beyond technical impossibility or infeasibility to include disproportionate effort, unreasonable or impracticable outcomes, and retention that is reasonably necessary for network, device, product, or service operation and improvement, complaint handling, regulatory or legal matters, security, fraud/scam prevention, and other legitimate public-interest purposes.

Broaden the fraud-prevention exception so that it clearly covers proactive activities reasonably necessary to prevent, detect, investigate, and remedy unlawful activity, or serious fraud/scam-related misconduct.

Ensure any revenue threshold for determining a large digital platform applies only local (Australian) service revenue for an individual service.

Provide appropriate safe harbours for intermediary technology.

7. PRECISE GEO-LOCATION DATA AND SENSITIVE INFORMATION

7.1 The ATA supports appropriate protection for precise geo-location and other sensitive information. The proposed definition and consent settings nevertheless require clarification and, in our view, amendment so that ordinary and necessary telecommunications functions are not inadvertently impeded.

7.2 Telecommunications networks, connected devices and associated digital services collect or generate location-related information, including precise geo-location – sometimes continuously - because that information is or may be needed to route traffic, establish and maintain connectivity, enable device or product functionality, manage networks and products, and provide the requested service. In those circumstances, location processing is an inherent feature of service or product delivery rather than a

separate tracking activity.

7.3 Similarly, ATA members may collect the location of premises and associated fixed or connected devices (e,g, routers, modems, appliances or other connected products) for the purposes of networks, device or product operations, maintenance, assurance, security etc. where the device is not being used to track the person's movements.

7.4 C/CSPs rely on the definition in section275A and the exceptions of Part 13, Division 3, of the *Telecommunications Act 1997* (Tel Act) that permit the disclosure or use of location data. Therefore, telecommunications network-based location data can only be used as permitted and authorised under Part 13 of the Tel Act and the *Telecommunications (Access and Interception) Act 1979* (TIA Act), and to the extent the data is only used in that way, it is taken to be authorised under the Privacy Act.

7.5 The proposed amendment to the Privacy Act seems to treat this information as personal information regardless of the Part 13 obligations on carriers, creating duplication of obligations.

7.6 C/CSPs and their employees and contractors seek clarification that they can rely on Division 4A of the Tel Act in respect of location information generated by a network in relation to devices registered to their networks. They seek clarification that collection of such data is considered a 'use' and, therefore, subject to the exemptions of the Tel Act.

7.7 They also seek clarification that where devices are being used by children and, consequently, precise geo-locations may be used (and collected), the proposed amendments do not create further duplication of obligations (between the Part 13 Tel Act and Privacy Act/Codes frameworks) for C/CSPs in respect of network-based device location information.

7.8 The proposed Privacy Act reforms will also apply to organisations outside the C/CSP context, including manufacturers of connected devices and providers of associated digital services that collect or process location information to provide product or service functionality. The strictly necessary' standard is too high and further information is required so organisations can assess whether a service or product's functionality is truly dependent upon geo-location data and whether a particular service could still be offered if that data is no longer collected, or could be provided with less precise geolocation data. The framework should recognise these different uses of location information and provide clear, workable rules for connected devices and associated digital services.

Recommendation 5

Clarify that the collection and use of location information reasonably necessary to provide, secure, maintain, or support a telecommunications service, connected device, product function, or associated digital service remains permitted, including where the service or product is used by a minor who is not the account holder or purchaser, and for fixed devices, products and premises.

Refine or authoritatively explain the 500-metre threshold so that it does not inadvertently treat the known location of fixed devices, products, or premises as precise geo-location tracking of an individual.

Provide clear guidance on when precise geo-location is necessary for product or service functionality, including the relevance of whether functionality can reasonably be provided using less precise location information.

8. DATA CONTROLLERS AND PROCESSORS

8.1 When enterprise clients use CPAS or other orchestration tools to collect, unify, and route data payloads to downstream analytics, CRM, or advertising destinations, these automated web-hooks risk being miscategorised as disclosures supporting direct marketing. Consequently, routine first-party data processing would be subjected to a rigid consent mandate under proposed APP 4.2.

8.2 Therefore, the proposed changes should completely operationally align with the Schedule 6 controller-processor framework. There should be explicit statutory text confirming that a cloud processor transmitting data solely on behalf of a controller to a destination specified under a documented contract is protected by a statutory carve-out and does not trigger trading consent rules.

8.3 This would ensure that accountability for direct marketing consent, and opt-out management rests entirely with the data controller initiating the campaign, rather than the underlying telecommunications API or cloud execution layer (who run e.g. two factor authentication).

Recommendation 6

> Insert a clear statutory boundary that distinguishes third-party consumer data brokers selling datasets from enterprise data pipelines executing first-party customer profile management.
>
> Explicitly exclude routine first-party data enablement, system integrations, and analytics routing from the trading definition.

9. DATA BREACH NOTIFICATIONS

9.1 The proposed 72-hour notification framework is one of the most operationally significant elements of the Bill. The ATA supports prompt notification where it enables regulators and individuals to take meaningful protective action, but the framework should distinguish speed from completeness and usefulness.

9.2 In a complex incident, an organisation may know within a short period that a serious event has occurred and that serious harm is foreseeable, while still being unable to identify which records were accessed, which customers are affected, or what protective steps are appropriate for particular individuals.

9.3 Forensic analysis of large and distributed data sets can take materially longer than 72 hours. Meaningful detail about affected records, threat-actor activity, and the scope of compromise may not be available during the initial response period.

9.4 Requiring notification to individuals before the affected cohort and relevant facts are sufficiently understood risks producing incomplete, alarming, or misleading communications. Organisations may feel compelled to notify every person who could possibly be affected, even where subsequent analysis substantially narrows the cohort.

9.5 Overly early notification may lead to initially notified individuals taking action, such as cancelling identification documents, which later may be found unnecessary but is irreversible.

9.6 The proposed approach also bears the risk of creating notification fatigue. Multiple early notices may make it less likely that customers recognise and act on a later communication containing specific protective guidance, while also creating avoidable public or market concern.

9.7 Early notice requirements also consume specialist resources during the most intensive phase of incident containment and investigation. Time spent preparing notices known to be incomplete can detract from remediation and from the work needed to establish facts that are most useful to affected individuals.

9.8 The regime should also avoid unnecessary duplication with cyber-security and critical-infrastructure incident reporting. Where multiple regulators require substantially similar early information, coordination and aligned reporting pathways should be used wherever practicable.

9.9 Notification to the OAIC and notification to affected individuals need not have identical triggers, content, or timing. A regulator can receive an early high-level report while the investigation continues; an individual notice should be sufficiently specific to explain the likely impact and any action the person can usefully take.

9.10 A staged model would better reflect incident response. An initial regulator notification could be made rapidly using information reasonably available at the time, with a high-level incident description and an express ability to supplement the notice as the investigation develops.

9.11 Further communications to clearly identified individuals should be required where there is material new information relevant to likely harm or protective action, rather than for every incremental development in the investigation.

Recommendation 7

Adopt a staged notification framework that distinguishes rapid notification to the OAIC from notification to affected individuals.

Initial regulator notices should contain information reasonably available at the time and be capable of supplementation.

Individual notification should be linked to the point at which affected people can be identified and sufficiently specific, useful protective information can be provided.

Require further individual updates only where material new information is relevant to likely harm or protective action.

10. MITIGATION OF HARMS

10.1 The ATA supports a duty to take reasonable steps to mitigate foreseeable harm following a privacy incident. For critical communications infrastructure, however, the duty must recognise that privacy harm may be only one of several 'competing harms' that require simultaneous management.

10.2 Measures that reduce confidentiality risk may adversely affect availability, integrity, or safety. Incident response decisions may therefore require trade-offs between protecting information and maintaining communications services, network stability, or access to emergency support.

10.3 For example, immediately disabling a compromised account may prevent further unauthorised access but may also deprive a customer of an essential communications service. The appropriate response may instead be to apply alternative controls while preserving continuity of service.

10.4 Prescriptive examples can be useful as guidance, but they should not operate in practice as mandatory steps irrespective of context. A measure that is appropriate in one incident may worsen the overall customer or public outcome in another.

10.5 Telecommunications providers may need to preserve emergency communications, critical service availability, and network integrity while containing a breach. These considerations are particularly important where the affected systems form part of critical infrastructure.

10.6 The statutory standard should therefore support proportionate decision-making across the full range of foreseeable harms, taking account of the seriousness and immediacy of the privacy risk, the availability of alternative controls, operational continuity, cyber security, safety, and public interest.

Recommendation 8

Frame the mitigation duty so that reasonable response measures may balance privacy risk against safety, cyber security, service availability, operational continuity, network integrity, and other foreseeable customer or public harms.

Require proportionate decision-making across confidentiality, integrity, and availability.

Avoid prescriptive requirements that could compel an action which reduces privacy risk but worsens the overall outcome.

11. IMPLEMENTATION LEAD TIME AND REGULATORY GUIDANCE

11.1 The proposed reforms would require material changes to data identification and classification, system and product controls, individual-rights processes, retention settings, breach-response procedures, governance arrangements, and staff training across large and complex telecommunications, device-manufacturing and digital service environments.

11.2 The combination of a broader and context-dependent data scope with new evaluative standards will be difficult to operationalise consistently without authoritative guidance. Industry will need sufficient time not only to amend policies but also to identify system dependencies, design and test controls, change customer and operational processes, and align implementation across overlapping regulatory regimes.

11.3 Guidance should be finalised well before commencement and should include detailed telecommunications, device manufacturer, and equipment supplier examples developed in consultation with industry. It should address, at a minimum, the expanded definition of personal information, APP 11 identification expectations, the fair and reasonable test, child-related factors and age assurance, access and erasure exceptions, precise geo-location, fraud prevention, breach notification, and harm mitigation. It should also appropriately consider emerging technologies and wearable devices.

11.4 A staged implementation approach may be appropriate where different obligations require different levels of system change. Commencement should allow regulated entities a realistic period to translate final legislation and guidance into tested operational processes rather than requiring major systems work against draft or unsettled requirements.

11.5 Implementation should also be coordinated across the OAIC and other relevant regulators so that guidance does not create inconsistent expectations for the same data, system or incident. Consistent cross-regulatory messaging will be particularly important for entities subject to telecommunications, cyber-security, and critical-infrastructure obligations.

11.6 Industry consultation during the implementation phase would assist in identifying practical issues early and in developing examples that improve consistency without undermining the principles-based character of the Privacy Act.

Recommendation 9

Provide an adequate transition period of at least 24 months, with staged commencement where appropriate, and publish final regulatory guidance sufficiently in advance of commencement to permit implementation.

Develop sector-specific telecommunications (including device manufacturer and equipment supplier) examples through consultation with industry and coordinate guidance across relevant regulators so that regulated entities can implement the reforms consistently with their existing telecommunications, consumer, cyber-security, critical-infrastructure and product obligations.

Ends

Australian
Telecommunications
Alliance

Level 25 / 100 Mount Street
North Sydney NSW 2060

T 02 9959 9111
E info@austelco.org.au
W austelco.org.au

ABN 56 078 026 507

