

Submission on Privacy Amendment (Personal Data Protection) Bill 2026

September 2026

ARC supports the objective of modernising Australia's privacy framework to better reflect the realities of the digital economy. We welcome reforms that are technology neutral, principled in design and capable of keeping pace with evolving data practices. Clear and timely guidance from the Office of the Australian Information Commissioner and adequate time for implementation (minimum two years) will be critical to ensuring compliance.

Fair and reasonable test and genuine choice

The new fair and reasonable test will require clear guidance on its practical applications. The key criteria should be laid out in legislation or explanatory materials, with practical supporting examples. Legitimate activities such as safety, fraud prevention, cybersecurity and crime prevention should be recognised when assessing whether a particular use of personal information is fair and reasonable.

The concept of 'genuine choice' is ill-defined, and its necessity unclear given existing consent requirements. APP 3.2(e) conflates choice about optional data uses with choice about handling, the latter being necessary to deliver the service the customer has requested. Retailers routinely handle personal information in ways that are inseparable from the service the customer has asked for. For example:

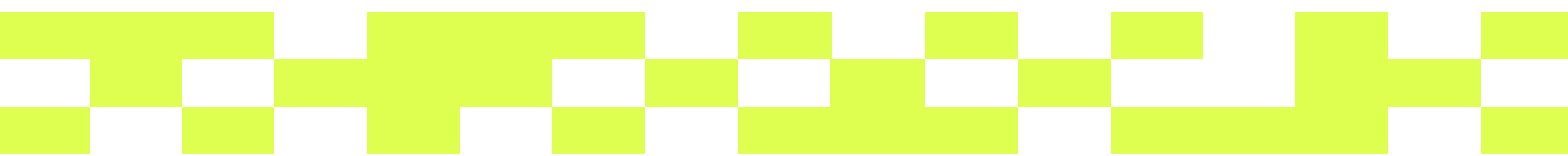
- **Delivery and logistics:** When a customer places an order for home delivery, the retailer must collect their address, share it with a carrier and track the parcel. There is no meaningful alternative to offer. The handling is the service.
- **Safety and security:** Retailers may use CCTV or other legal security measures to prevent theft, keep customers and staff safe. Along with appropriate safeguards and a privacy impact assessment, this should be sufficient to demonstrate the activity is fair and reasonable, 'genuine choice' has no practical application.

We recommend that 'genuine choice' is limited to optional or secondary uses of personal information. As an alternative, we recommend the introduction of a contract-necessity basis (or statutory safe harbour) confirming that handling reasonably necessary to provide a requested product or service satisfies the fair and reasonable test. This could include handling: 1) clearly disclosed to the individual; 2) necessary to provide or support a product or service the individual has requested; and 3) consistent with reasonable expectations in that context.

Direct marketing

The proposed definition of direct marketing risks capturing activities that are part of the core features of a retail service itself. Product recommendations and personalised search results are not only integral to how customers shop but are also an expected part of the shopping experience.

We recommend amending the definition to "promotional or commercial intent to sell goods or services external to the service the customer is already using". This confirms that key service features and contextual suggestions offered by a retailer within their own service are not classified under this definition.



Further, while the opt-out requirements are appropriate for emails and text messages that can include a very clear “unsubscribe” button, it is problematic for aspects of personalised advertising like website banners, which cannot practically include this in the same manner. It is also important that these opt-out services do not disable settings that allow the retailer’s product to function, such as order confirmations and delivery notifications.

We recommend making the ability to opt-out prominent and accessible at the account/service level, rather than with each individual communication, and clearly delineating between targeted advertising and service functionality. This maintains the integrity and intent of the opt-out function, while avoiding an unnecessary reduction in the customer’s chosen service.

Transparency and data trading

Clarification is requested regarding the reference in the fair and reasonable test to providing transparency about the means and purposes of data collection, use and disclosure. The scope of these requirements, particularly with respect to the means of data collection is unclear. Will entities be compelled to provide unnecessary technical detail about their information processing activities? Retailers may use automated systems for such things as inventory management, fraud detection and product recommendations, and the potential imposition of these disclosure obligations will be substantial.

The definition of ‘trading’ is ambiguous. There should be a clear ability to distinguish between ordinary retailing activities including communicating with existing customers and delivering on expected services like first-party value exchange arrangements and selling personal information. We recommend aligning this definition with the existing Spam Act and Do Not Call requirements, to alleviate against unnecessary complexity.

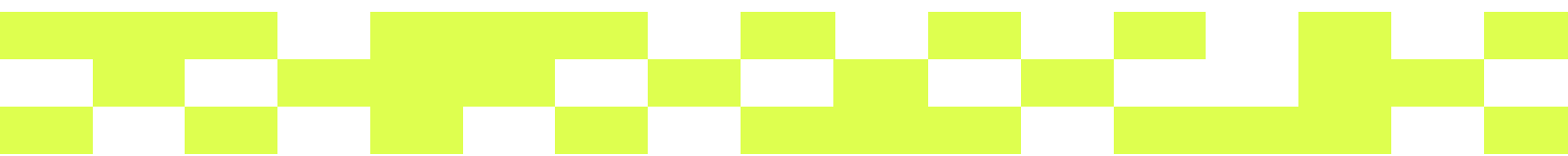
Security and data breaches

ARC members do not oppose the principle of the 72-hour notification timeframe. However, a simultaneous 72-hour notification to customers takes resources away from the priority, which must be incident containment and correction. Notifying customers early and without confirmed facts is fraught with risk, as it is often impossible to accurately scope the incident in this timeframe. Inaccurate communications may require subsequent correction and erode trust with consumers.

We recommend starting the 72-hours once there are reasonable grounds to believe a notifiable breach has occurred, rather than when the incident is first identified. Combined with the ability to submit preliminary notifications, this solution would further improve the veracity and timeliness of reporting of security breaches. For example, if a cyber incident occurs with a supplier and the retailer is notified, but there is initially no evidence customer information has been affected, there should be scope to conduct a practical assessment and investigation of the breach and subsequently provide customers with relevant and accurate information.

Transitional period

ARC notes the broad scale of these reforms. Entities will need to update privacy policies and practices, requiring significant time and resources. Updates may be required to systems, contracts, privacy notices and broader governance processes with these reforms. We recommend a transition period of two years, from the publication of any OAIC guidance and supporting rules. This would provide organisations with sufficient certainty regarding regulatory expectations and enable meaningful implementation planning. Experience with recent reforms has demonstrated the importance of timely guidance to support compliance with new obligations and avoid organisations having to implement significant changes in advance of settled regulatory expectations.



Additionally, where existing entities are complying with current APPs, consideration should be given to a safe harbour protection, such that there is not a need to re-evaluate existing processes when legislative practices are being met.

Emerging technologies

Retailers and their team members engage with members of the public every day. In that environment, emerging technologies such as smart glasses present new and significant privacy risks for customers and retail workers alike, particularly where they enable recording without notice, transparency or consent.

In one recent example, a retail team member was covertly recorded by a member of the public wearing smart glasses during an ordinary in-store service interaction. The customer subsequently uploaded the footage to TikTok. The team member was not aware they had been filmed and did not know the footage had been shared publicly on social media. While this conduct may fall outside the current scope of the Privacy Act, the impact on the individual was significant. They were denied the opportunity to consent to the collection of their image and lost control over how their image, and therefore their personal information, was used and disclosed.

This example highlights a clear gap in the current legal framework, particularly given the consultation paper's recognition of the privacy risks posed by emerging technologies. The gap is especially apparent when compared with the clearer rules that apply to listening devices. We recommend that the Government and the OAIC consider targeted policy reform, guidance or other practical measures to address covert recording through smart glasses and similar technologies. Without reform, the law risks falling further behind emerging forms of recording and disclosure that can cause real harm to individuals. ARC would welcome the opportunity to work with the OAIC and Government on options to provide greater certainty and protection for individuals in public-facing settings.

Please contact policy@retail.org.au if you have any questions about this submission.

About ARC

ARC represents the Australian retail sector. Valued at \$444 billion, retail is the nation's largest private sector employer, supporting more than 1.5 million jobs, including more young Australians aged 15 to 24 years than any other industry. ARC's membership is diverse. From family-owned small and independent businesses, comprising 95 per cent of our membership, to large national and international retailers supporting communities across metropolitan and regional Australia. With more than 155,000 retail outlets nationwide and a growing online presence, the retail sector is embedded throughout the economy, playing a critical role in the supply chain of Australian businesses. ARC advocates for policies and reform that drive growth, resilience, and long-term prosperity for Australian retail and the millions who rely on it. At a time of rapid change, from technological disruption and international competition to shifting consumer behaviour and sustainability expectations, effective policy settings are critical for retailers, workers, consumers, and communities.