ARA/NRA SUBMISSION

PILLAR 3: HARNESSING DATA AND DIGITAL TECHNOLOGY

JUNE 2025

The Australian Retailers Association (ARA) and National Retail Association (NRA) welcome the opportunity to contribute to the Productivity Commission's consultation on *Pillar 3: Harnessing Data and Digital Technology* – a critical area for unlocking innovation, improving service delivery, and lifting national productivity through smarter regulation and digital transformation.

The ARA and NRA, which propose to amalgamate into the Australian Retail Council (ARC), represent a **$430 billion sector,** and employs **1.4 million Australians** – making retail the largest private sector employer in the country and a significant contributor to the Australian economy.

Our membership spans the full spectrum of Australian retail, from family-owned small and independent retailers that make up 95% of our membership, through to our largest national and international retailers that employ thousands of Australians and support both metropolitan and regional communities every day.

With a significant portion of every dollar spent in retail flowing back to employees, suppliers, super funds, and local communities, a thriving retail sector benefits all Australians. After a uniquely challenging five-year period, which has had significant impacts on the sector, we are united in advocating for policies, reform and collaboration that will drive growth, resilience, and prosperity for the retail sector and all Australians.

EXECUTIVE SUMMARY

As Australia seeks to boost national productivity, the retail sector stands ready to contribute through accelerated adoption of digital technologies, particularly artificial intelligence (AI) and data-driven innovation. Retailers are already using AI to optimise operations, personalise customer engagement, and improve staff safety. These tools are also becoming increasingly important in reducing retail crime, which imposes an estimated $9 billion annual cost on the economy and accounts for 2.3% of merchandise loss, adding significant pressure to already tight margins.

At the same time, the responsible handling of personal data is fundamental to building and maintaining consumer trust across increasingly integrated physical and digital environments.

The Government's ongoing efforts to modernise AI governance and reform the Privacy Act are timely and welcome. However, these reforms must be designed to support innovation as well as protection. Many retailers are small to mid-sized businesses and end-users of third-party systems, not developers of AI models or custodians of large data science teams. Regulatory approaches that fail to account for this reality risk placing disproportionate burdens on businesses that lack the scale or technical control to meet prescriptive obligations.

The focus of this submission is on two priority areas where there is the greatest opportunity to lift retail productivity through more proportionate and productivity-enhancing digital policy:

- Supporting Safe Data Access and Handling through an Outcomes-Based Approach to Privacy, and

- Enabling AI's Productivity Potential.

SUPPORT SAFE DATA ACCESS AND HANDLING THROUGH AN OUTCOMES-BASED APPROACH TO PRIVACY

Retailers engage with millions of Australians each day; in stores, online, and across digital platforms, making privacy compliance not just a legal requirement, but central to maintaining customer trust. From e-commerce transactions and loyalty programs to targeted marketing, personal information has become essential to delivering secure, seamless, and personalised retail experiences.

However, the nature and volume of data held by retailers has evolved dramatically since the Act's inception. The retail sector now sits at the intersection of consumer behaviour, digital innovation, and public scrutiny, prompting strong interest in the Federal Government's ongoing review and reform of the Privacy Act.

Retailers broadly support the modernisation of the Privacy Act to reflect the realities of the digital economy and align with contemporary community expectations. However, there is a need to ensure that reforms are balanced, practical, and proportionate, protecting individuals without imposing unreasonable compliance burdens or inadvertently restricting retailers' ability to provide safe, efficient, and innovative services.

Some aspects of the Privacy Act, particularly around consent, exemptions and procedural requirements, have created uncertainty for businesses, especially with technologies including facial recognition technology (FRT). The interpretations of the current regime have limited the ability of businesses to use enhanced technology offerings and initiatives to improve safety outcomes for team members and customers, even where privacy risks were minimal and mitigated.

Facial recognition technology (FRT) has shown potential for deterring and addressing retail crime in international markets, including the UK and New Zealand. However, its use in Australia remains legally unclear due to uncertainty surrounding the Privacy Act 1988. The Act classifies biometric data, including facial images, as sensitive information, leading to ambiguity around how it can be lawfully collected and used in retail settings. The absence of a specific legal framework for FRT in retail settings creates operational uncertainty and exposes retailers to potential regulatory challenges.

The ARA and NRA strongly support the responsible adoption of FRT as part of a comprehensive strategy to reduce retail crime and improve staff and customer safety.

The original intention of the privacy principles must be adhered to, as outcomes-based privacy obligations can ensure businesses can deliver better safety and service outcomes while protecting and respecting customers and their personal information. We believe that it is possible to deliver strong privacy protections and focus on outcomes including fairness, secure data handling and transparency. Notice and disclosure fatigue can diminish customer experience, and we urge the Federal Government to consider reform that balances the objectives of the Privacy Act, while ensuring businesses can operate effectively.

The Privacy Act has served Australia well since its extension to the private sector in 2001, with its technology-neutral, principles-based approach remaining relevant amid evolving technology and work practices. However, recent interpretations of privacy regulation have shifted toward prescriptive compliance methods, creating uncertainty and hindering businesses from operating effectively. We support a move to an outcomes-based approach, with clearer guidance for organizations deploying new technologies. Regulators should focus on interpretation, guidance, and direction rather than advocacy, ensuring reasonable and compliant positions do not

lead to uncertain outcomes. This balance would build public trust while giving businesses the clarity and flexibility to use data for improved productivity, customer experience, and responsible innovation in service, efficiency, and safety, including technologies like facial recognition in well-defined, safety-related contexts with strict safeguards and low privacy risks.

Additionally, we propose specific updates to the Privacy Act. First, the employee records exemption has been narrowly interpreted by courts, reducing its relevance as employees are often also customers whose personal information deserves equal treatment. Removing this exemption could align Australia with global standards, such as the EU's data protection laws, enhancing efficiency in handling all personal information consistently.

Second, the Act should address retention and destruction, an area not fully contemplated in the era of paper records. With the volume of data generated daily across multiple channels, clearer, technology-agnostic guardrails are needed for appropriate retention periods and methods for de-identifying or masking data. This outcomes-based approach would create consistent expectations across the ecosystem, supporting both consumer protection and business innovation.

Background

Retailers face uncertainty due to overlapping and sometimes contradictory requirements across regulatory frameworks. For example, the Privacy Act's data minimisation principle is at odds with obligations under the Corporations Act, AML/CTF legislation, and workplace safety laws, which require retailers to retain personal data for extended periods. There is also a lack of clarity around what constitutes "reasonably necessary" data collection particularly in high-traffic retail settings where businesses must consider staff safety, incident reporting, or security analytics.

In addition, public trust in digital technologies depends on informed consent and transparency in data handling. Strengthening audit capabilities, ensuring interoperability across government systems, and addressing cross-border data flow concerns are all part of building a fit-for-purpose privacy regime that supports innovation without compromising accountability.

Uncertainty extends to the use of AI and biometric technologies. Many retailers are exploring or trialling tools like facial recognition and behavioural analytics to improve safety and service delivery, but operate cautiously due to unclear expectations around consent, proportionality, and regulatory oversight. Without clear guidance, businesses face a chilling effect on innovation, even where community benefit and safety outcomes are strong.

The complexity is especially burdensome for small and medium retailers, many of whom lack internal privacy or legal teams. The proposed removal of the small business exemption would exacerbate this issue, imposing disproportionate costs on low-risk operators at a time when regulatory simplification is being pursued internationally.

Recommendations

An outcomes-based privacy framework would give businesses the flexibility to implement controls proportionate to their operations and risk profile, without undermining consumer protection. To support this approach, we recommend:

- Retaining the small business exemption to ensure regulatory obligations are proportionate and aligned with international best practice;
- Providing clear, sector-specific guidance on what constitutes "reasonably necessary" data use, including defined permitted purposes such as loss prevention, staff safety, and customer experience;

- Harmonising privacy obligations with intersecting laws, including cybersecurity, data retention, workplace health and safety, and surveillance legislation, to reduce duplication and legal uncertainty;
- Introducing safe harbour protections for businesses that adopt approved codes or industry standards, enabling innovation with compliance confidence.

ENABLE AI'S PRODUCTIVITY POTENTIAL

AI is already transforming retail, from personalised marketing and predictive inventory management to workforce rostering, fraud detection, and customer service automation. These technologies are delivering measurable gains in efficiency, customer experience, and decision-making, making AI an increasingly embedded part of the modern retail operating environment.

As AI adoption accelerates, it is essential that regulatory settings support innovation while ensuring public trust, transparency, and accountability. The retail sector broadly welcomes the Government's intention to develop a safe, coordinated approach to AI governance, particularly in high-risk settings. However, most retail AI use cases are low to moderate in risk and are not used for decisions with significant legal, financial, or reputational consequences. Applying a one-size-fits-all regulatory model risks imposing disproportionate compliance burdens, especially for small and medium-sized retailers who are often end users of third-party tools.

This section outlines the retail sector's perspectives on enabling AI's productivity potential in a way that balances safety with innovation. While the ARA and NRA have previously commented on broader AI policy and regulatory proposals, including the Government's guardrails for high-risk AI, this paper focuses specifically on the questions raised in the Productivity Commission's consultation.

Background
Retailers across Australia are already deploying AI to improve operations, enhance service delivery, and respond to customer needs in real time. Current use cases include product recommendation engines, demand forecasting, chatbot support, loss prevention analytics, and automated staff rostering. Looking ahead, the sector sees significant additional upside from expanding AI capability across three key areas:

- **Colleague Safety and Incident Prevention**: Facial recognition technology (FRT) is being explored by retailers, as a tool to identify known repeat offenders and support early intervention in incidents of theft or customer aggression. In the context of rising retail crime, AI-enabled FRT offers a way to enhance staff safety by detecting threats in real time and reducing reliance on reactive measures. This technology complements manual monitoring and can form part of a broader safety strategy when used responsibly and transparently.

- **Increased Productivity and Resource Allocation**: Retailers are exploring AI for real-time workforce management, automated compliance tracking, and energy optimisation within stores and distribution centres. For example, AI could help dynamically adjust lighting, air conditioning, or equipment maintenance schedules based on usage patterns, cutting costs and reducing environmental impact. At a strategic level, AI will increasingly inform category management, supply chain routing, and omnichannel optimisation.

- **Customer Experiences**: From predictive search and visual product recognition to individualised loyalty rewards and hyper-personalised marketing, AI is helping retailers deliver more relevant, timely, and frictionless customer interactions. As consumers come to expect tailored services across both online and physical environments, AI is key to meeting that expectation at scale.

Despite these benefits, retailers face a number of practical and policy challenges in realising AI's full productivity potential, particularly in navigating regulatory complexity, legal uncertainty, and uneven access to AI capability. These are explored in the following section.

Challenges

While the potential of AI in retail is substantial, several challenges limit the sector's ability to fully embrace AI technologies in a safe, productive, and scalable way.

The proliferation of parallel policy processes, including the proposed guardrails for high-risk AI, reforms to the Privacy Act, cyber security obligations, and digital platform regulations, is already creating uncertainty. Retailers face a growing patchwork of obligations that often lack clarity, alignment, or proportionality. This environment is especially challenging for small and mid-sized businesses that rely on third-party AI tools and have limited internal compliance capacity.

Secondly, the compliance burden of proposed AI frameworks could be unsustainable for SMEs. Requirements such as formal risk assessments, audit trails, and conformity assessments are not feasible for businesses using plug-and-play solutions for rostering, customer service, or inventory management. Without scaled obligations or tailored support, innovation at the SME level may stagnate.

Finally, there is no mechanism to support real-world testing or responsible exploration of new AI tools. Without a regulatory sandbox or clear testing pathway, retailers face an "all-or-nothing" compliance model that discourages experimentation and delays productivity gains.

Further challenges include ethical concerns such as bias and explainability in AI decision-making, especially in systems influencing staffing, marketing, or product access. While most retail AI applications are low-risk, clearer national guidance on ethical use, including transparency obligations and data training standards (e.g. copyright or personal data), would assist retailers in navigating compliance with confidence.

Recommendations

To unlock the productivity potential of AI while maintaining trust and accountability, Australia's AI regulatory approach must be risk-based, proportionate, and supportive of innovation. The following recommendations reflect what is most needed to enable responsible AI use in the retail sector:

1. **Adopt a risk-tiered framework**
   Regulation should reflect the level of risk posed by the AI application. Low-risk tools commonly used in retail such as product recommendations, rostering, and customer service chatbots should not carry the same obligations as high-risk AI used in areas like recruitment or law enforcement. This model is consistent with international best practice, such as the EU AI Act's four-tier risk classification.

2. **Align AI obligations with existing laws and ethical frameworks**
   AI regulation should integrate with existing legal and ethical obligations, including the Privacy Act, consumer law, cybersecurity requirements, and voluntary AI ethics principles, to reduce duplication and provide clarity. Particular attention should be given to harmonising rules around liability, consent, and algorithmic explainability.

3. **Support SMEs with tailored pathways**
   Small and medium-sized retailers should not be expected to meet the same regulatory burden as large tech companies or AI developers. Simplified compliance options, template tools, and targeted support

must be made available, particularly for businesses that use third-party AI products without the ability to access or alter system design. In parallel, greater investment in digital literacy and capability-building is essential, especially for small businesses and those operating in regional areas. Ensuring equitable access to digital skills and tools will help prevent Australia's digital divide from widening and ensure all retailers can participate in the benefits of digital transformation.

4. **Introduce a regulatory sandbox for AI innovation**
   A sandbox model would enable businesses to test AI solutions in partnership with regulators under controlled conditions. This encourages safe experimentation, supports capability building, and helps inform regulatory design with real-world insight. It is especially valuable for emerging use cases in retail such as AI-assisted recruitment or store safety systems.

5. **Ensure proportionate transparency and accountability requirements**
   Retailers should inform customers and employees when AI is used in decisions that materially affect them, but requirements should be context appropriate. Overly prescriptive obligations may deter beneficial uses or create 'consent fatigue' without improving outcomes.

RECOMMENDATIONS

To unlock productivity gains while maintaining public trust and regulatory clarity, the Australian Government should adopt a coordinated and principle-based approach to both AI regulation and privacy reform. These frameworks must evolve in parallel, recognising their interdependence and cumulative impact on businesses. The retail sector recommends that future policy and legislative design be guided by the following overarching principles:

1. Ensure regulatory consistency across AI, privacy, cyber, and consumer law to avoid duplication and conflicting obligations.
2. Adopt a risk-based approach that scales compliance requirements according to actual use and impact.
3. Support SMEs through simplified obligations, exemptions, and tailored compliance tools.
4. Enable innovation via sandboxes, safe harbour provisions, and flexible, outcome-focused standards.
5. Provide clear guidance on retail-specific issues like data use, consent, and biometric technologies.

As Australia enters a new wave of digital transformation, data governance, consumer empowerment, and AI readiness will be central to lifting national productivity. The retail sector is at the forefront of these changes and is committed to working with government to ensure regulation supports growth, innovation and public confidence.

We welcome the opportunity to contribute further to this process and assist in the implementation of practical, scalable reforms.

Thank you again for the opportunity to provide a submission on *Pillar 3: Harnessing Data and Digital Technology*. Any queries in relation to this submission can be directed to our policy team at policy@retail.org.au.