Australian Retailers Association

SUBMISSION
PRIVACY ACT REVIEW

MARCH 2023

EXECUTIVE SUMMARY

The Australian Retailers Association (ARA) supports a review of the Commonwealth Privacy Act, in line with the guiding principles and comments outlined in this submission. We note the wide-ranging nature of the government's review but will focus on response on those proposals that are most relevant to the Australian retail sector.

INTRODUCTION

The ARA is the oldest, largest and most diverse national retail body, representing a $400 billion sector that employs 1.3 million Australians – making retail the largest private sector employer in the country. As Australia's peak retail body, representing more than 120,000 retail shop fronts and online stores, the ARA informs, advocates, educates, protects and unifies our independent, national and international retail community.

We represent the full spectrum of Australian retail, from our largest national retailers to our small and medium sized members, who make up 95% of our membership. Our members operate across the country and in all categories - from food to fashion, hairdressing to hardware, and everything in between.

The ARA welcomes the opportunity to comment on the proposed reforms to the Privacy Act (the Act). ARA members understand that privacy is key to maintaining customer trust and its social licence to continue using personal information to provide customers with innovative and valuable personalised shopping experiences.

We note the comprehensive nature of the review but will focus our response on those proposals that have a direct impact or consideration for the retail sector.

GUIDING PRINCIPLES

Beyond those proposals that the ARA will comment on in this submission, we recommend that government considers the following principles when developing its response to the Privacy Act Review.

- Reforms should be in line with community expectations about privacy
- Reforms should not impose an unreasonable compliance burden on businesses
- Reforms should not prevent businesses from collecting, using and retaining personal information for safety and security reasons
- Reforms should not unreasonably restrict customer access to products and services of interest to them
- Reforms should avoid burdening customers with excessive information and creating consent fatigue
- Explanations of business obligations should be clear, concise and available in plain English
- Businesses should be given appropriate lead time (12-24 months) to prepare for the changes
- Reforms should consider learnings from other jurisdictions that have implemented enhanced privacy settings
- Reforms should be in line with international best practice but not go beyond it.

Australian Retailers Association (ABN 99 064 713 718)
Level 1, 112 Wellington Parade, East Melbourne VIC 3002

Australian Retailers Association

ARA COMMENTS ON SPECIFIC PROPOSALS

As noted, the ARA will not be providing comment on all 116 proposals outlined by the review. We limit our commentary to the following proposals that have an impact or consideration for the retail sector.

4.1 Changes affecting the definition of personal information

4.9 Changes affecting the definition of sensitive information

6.1 Removal of the small business exemption

7.1 Enhanced protections for employee records

11.1 Definition of consent

11.2 Standardised consent requests

11.4 Requirement for default online privacy settings

18.0 Introduction of rights of the individual

15.2 Requirement to appoint a senior employee responsible for privacy

20.1 Definitions of direct marketing and targeting

20.2 Requirement for an unqualified right to opt-out of direct marketing

20.3 Requirement for an unqualified right to opt-out of targeted advertising

20.8 Addition of prohibitions to targeting individuals based on sensitive information.

Proposal 4.1
Changes affecting definition of personal information

The ARA submits that the current definition of personal information in the Act is sufficient to provide privacy protection in line with community expectations. The final report recommends changing the word “about” to “relates to” in the definition of personal information so that data like IP addresses and device identifiers are captured in the definition.

We are concerned that, if Australian Privacy Principal 5 (notification of collection of personal information) were to be applied to the collection of IP addresses and device identifiers, customers shopping online or participating in customer loyalty programs would be overwhelmed by collection notices. This could deter them from participating in these activities but also make it less likely for them to engage with more important notices regarding their privacy.

The ARA therefore recommends maintaining the current definition of personal information and creating separate protections for data if determined necessary.

Proposal 4.9
Changes affecting definition of sensitive information

The ARA recognises the need to apply extra care and caution to the handling of individuals’ sensitive information. However, we are concerned with the compliance implications of the proposal to “clarify in the Act that sensitive information can be inferred from information that is not sensitive information.”

Shopping patterns can infer sensitive information about an individual, including physical health, mental health, sexuality, and religious/political beliefs, but it is difficult to determine at what point a series of transactions reasonably infers that sensitive information. For example, how many times and how frequently does an individual need to purchase pregnancy and/ or infant items for it to be inferred that they are pregnant?

Australian Retailers Association (ABN 99 064 713 718)
Level 1, 112 Wellington Parade, East Melbourne VIC 3002

This could prove particularly problematic in complying with proposal 20.8, which proposes to ban targeting individuals based on sensitive information. For example, customer loyalty programs routinely use transaction history to present participants with offers of interest to them. Could this practice then be prohibited in circumstances where an individual's transaction history reveals sensitive information?

The ARA recommends that government provide further guidance to avoid inadvertent non-compliance.

Proposal 6.1
Removal of the small business exemption

The ARA agrees that Australians should expect their personal information to be protected regardless of the size of the business that collects that information. We also understand that with most small businesses now trading online, there is a greater risk of the personal information collected by these businesses being compromised.

However, businesses of all sizes must be able to understand and comply with relevant regulations, including small and medium sized businesses, the proposed changes are to achieve their stated purpose of protecting personal information.

Unlike their larger counterparts, small retailers typically don't have access to the legal or technological expertise required to interpret privacy legislation. Acute labour shortages in the retail sector mean they have even less time to devote to compliance.

In a survey of ARA small business members, 61% of respondents rated their current understanding of the Privacy Act and Australian Privacy Principles as "poor" or "very poor." More than half said that they didn't understand what was expected of them in creating a privacy policy. Respondents also said that the resources most helpful to them would be written guidance tailored to small businesses, compliance checklists, and templates for privacy policies and collection notices.

The ARA therefore supports the proposal to conduct an impact analysis and undertake additional consultation with small businesses before removing the exemption. The impact analysis must include the financial impact of both initial and ongoing compliance.

Proposal 7.1
Enhanced protections for employee records

The ARA is supportive of protecting the privacy of employee data in the same way that other data is currently protected but has some concerns about practical application when it comes to consent, right to access and right to erasure.

The ARA therefore recommends that the current exemption for employee records be retained in the Privacy Act. However, we would welcome further opportunities to consult on enhanced protections for employee records that balance the employees need for privacy against the business needs to manage its operations efficiently.

Proposal 11.1
Definition of consent

The ARA is concerned about the ambiguity of the word "current." It implies that consent can expire but does not specify any timeframes. The ARA therefore recommends that government provide clarity on how often entities are expected to ask for consent. We recommend that this be no more frequently than yearly.

Australian Retailers Association (ABN 99 064 713 718)
Level 1, 112 Wellington Parade, East Melbourne VIC 3002

Proposal 11.2
Standardised consent requests

While creating guidance for standard consent requests would be very helpful to SMEs – especially those that have not previously been covered by the Privacy Act – some ARA members with global operations have already developed their own consent requests that can be used across multiple jurisdictions.

Having a prescriptive approach in Australia would increase the compliance burden on these businesses without necessarily having a meaningful impact on privacy. The ARA therefore supports the proposal to create guidance for standard consent requests, but recommends that this guidance be voluntary, not mandatory.

Proposal 11.4
Requirement for default online privacy settings

Many business groups were opposed to the proposal in the discussion paper that would require entities to select the "most restrictive" privacy settings, but the proposal in the final report that "privacy settings should reflect the privacy by default framework of the Act" is unclear. The final report explains that "the Act requires that only personal information and sensitive information that is reasonably necessary (or 'directly related' for agencies) for an entity's functions or activities may be collected."

The ARA recommends that government provide a clearer definition of default privacy settings but would be broadly supportive of changing default privacy settings to what is "reasonably necessary for an entity's functions."

Proposal 18
Introduction of rights of the individual

The ARA supports the intention behind these rights but has some practical concerns, particularly regarding the right to erasure. We support the proposed exceptions but submit that there should be an additional exception for legitimate business security interests because "public interests" does not necessarily cover circumstances where complying with a request to erase personal information would interfere with business activities to keep customers, employees and business assets safe.

Complying with a request to erase personal information could be contrary to what the customer wishes to achieve by exercising this right. In order to follow customer requests not to be contacted for marketing purposes, some sort of record needs to be kept. For example, that person's email address and phone number may be added to a 'do not contact' list. Without that, there is a risk that the person will be contacted again if the business obtains that person's information from a different source.

Another concern is that the right to access and explanation is duplicating requirements that already exist under APP 5, increasing the compliance burden on businesses without providing any additional privacy benefits to individuals. APP 5.2 requires entities to ensure individuals are aware of the purposes for which their personal information is being collected.

Additionally, complying with requests to exercise rights of the individual could be particularly burdensome for small retailers, especially if there is only one staff member with access to customers' personal information (as is often the case). Before removing the small business exemption, consideration should be given to whether the burden on small businesses outweighs the privacy benefits to the individual for each of the proposed rights in Chapter 18.

This may not be the case for erasing or correcting someone's personal information but would likely be the case for requiring businesses to acknowledge the receipt of a request and respond in writing to customers exercising their right to object (proposals 18.1 and 18.2). Would the exemption for requests that are "unreasonable" cover cases where small businesses don't have time to respond?

Australian Retailers Association (ABN 99 064 713 718)
Level 1, 112 Wellington Parade, East Melbourne VIC 3002

In summary, the ARA recommends that:

- An additional exception be created for legitimate business interests
- Remove the requirement to provide an explanation under proposal 18.1
- For each of these proposed rights, consideration be given to whether the burden on small businesses outweighs the privacy benefits to the individual.

Proposal 15.2
Requirement to appoint a senior employee responsible for privacy

While this proposal will have little impact on medium and large retailers, it is unworkable for small retailers that have few employees. Employees of small retailers, many of whom are young and work part time, should not be expected to have the skills or knowledge required to be responsible for privacy.

The ARA agrees with the final report's assertion that "consideration should be given to excepting or modifying this requirement for some small APP entities that are covered by the Act where they are less able to absorb its associated regulatory costs."

The ARA recommends that small businesses be exempted from this proposal or, failing that, modify the wording to allow the business owner to be responsible for privacy rather than a senior employee.

Proposal 20.1
Definitions of direct marketing and targeting

While we support the intention to create a distinction between direct marketing and targeting, the proposed definitions in the final report are not distinct enough. The proposed definition of targeting is so broad that it may also capture some direct marketing, making it difficult for businesses to comply with opt-out requests and for customers to know what they are opting out of. For example, it is common practice for marketing emails to include the subscriber's name in the greeting line – as this is tailoring content based on personal information, this would be captured in the proposed definition of targeting.

The broad definition of targeting poses additional problems. For example, device identifiers are "information relating to an individual." Under the proposed definition, using device identifiers to tailor website content so that it is readable on the type of device being used (i.e. desktop or mobile) would be considered targeting. Customers opting out of targeting because they do not wish to receive personalised advertisements would be unnecessarily inconvenienced.

The ARA therefore recommends that the proposed definitions of direct marketing and targeting be refined to ensure they capture distinct activities and are mutually exclusive so that if a customer opts out of one, they do not inadvertently opt out of both.

Proposal 20.2
Requirements for an unqualified right to opt-out for direct marketing purposes

Business groups were opposed to the proposal in the discussion paper, which was for an unqualified right to opt-out of the collection, use and disclosure of personal information for direct marketing purposes because the purpose of personal information is not always known at the point of collection.

The ARA supports the revised right in the final report which removes the word "collection." We agree that individuals should be able to opt-out of receiving direct marketing.

Australian Retailers Association (ABN 99 064 713 718)
Level 1, 112 Wellington Parade, East Melbourne VIC 3002

Proposal 20.3
Requirement for an unqualified right to opt-out of targeted advertising

As discussed under proposal 20.1, the broad definition of targeting could make it difficult for customers to know what they are opting out of. The definition of targeting needs to be refined for this proposal to be useful.

Additionally, some ARA members have expressed concern about how this proposal may affect the functionality of their customer loyalty programs. While not in the list of proposals, the final report states on pages 211 and 214 that exercising this right to opt-out "should not be a barrier to service."

It is unclear whether the intention is to require retailers to allow customers to continue to participate in customer loyalty programs after opting out of receiving direct marketing and/or targeted advertising, both of which are key features of customer loyalty programs.

It is the view of these ARA members that customer loyalty programs are mutually beneficial to customers and retailers, with customers receiving discounts and tailored offers in exchange for providing retailers data.

These ARA members are concerned about the potential cost of having to design a second version of their loyalty schemes to cater to customers who do not wish to receive direct marketing and/ or targeted advertising.

While the ARA agrees that opting out of targeted advertising should not be a barrier to receiving essential services (such as using the internet), we believe it is reasonable to make targeting advertising a condition of participating in a customer loyalty program. The ARA therefore recommends that the government allow entities to make receiving targeted advertising a condition of service if a key component of that service is targeted advertising, as is the case with customer loyalty programs.

Proposal 20.8
Addition of prohibition of targeting individuals based on sensitive information

As noted in the submission, the ARA seeks further guidance on this proposal and whether it would extend to targeting based on inferred sensitive information. It is difficult to determine at what point a string of non-sensitive information (such as transactions) can reasonably infer sensitive information about a customer and therefore at what point targeting would be prohibited.

We are concerned that, without further guidance, this proposal could expose retailers to complaints from customers who believe they are being targeted based on sensitive information.

The ARA recommends that government provide further guidance to avoid inadvertent non-compliance.

The ARA appreciates the opportunity to provide feedback on this review and looks forward to further engagement as the government develops its official response.

For any questions about this submission please contact policy@retail.org.au.

Australian Retailers Association (ABN 99 064 713 718)
Level 1, 112 Wellington Parade, East Melbourne VIC 3002