Submission on

Australian Government's Response to Privacy Act Review

on behalf of

Australian Association of National Advertisers

April 2023

Introduction

AANA is the peak body for advertisers and exists to promote all forms of responsible marketing through the self-regulation of advertising content to ensure it meets prevailing community standards.

Since 1997 the AANA and Ad Standards have been the custodian of Australia's advertising content self-regulation system, successfully developing advertising codes and operating an impartial complaint handling process with a high compliance rate at no cost to tax-payers. The advertising self-regulatory system was established in recognition of advertisers' responsibility to deliver marketing that is aligned to community standards and expectations. The rules apply to all advertising, including online advertising, and prohibit the advertising of certain products such as alcohol, gambling and occasional foods to children (under 15 years) and minors (under 18 years). In relation to online advertising, targeting tools are used to ensure compliance with these rules.

The advertising, marketing and media industry plays a fundamental economic role in society - contributing approximately $40 billion to the Australian economy and employing over 200,000 people[1]. It is the driver of consumer choice and, by promoting competition, helps consumers get better value for money. It enables innovation to be brought to market and stimulates economic growth and jobs.

Advertising also plays a crucial role in funding free access to news, free to air television, free digital entertainment, music, email, social media and other media services as well as subsidising the cost of public transport infrastructure.

Summary

AANA supports the proposals contained in the Australian government's response, with two exceptions:

- The proposals that restrict targeted marketing, especially to children, may have the unintended consequence of ensuring that children and vulnerable groups see advertising they should not, such as advertising for alcohol, gambling and occasional food or drinks. AANA believes that use of targeting data to exclude such groups from seeing inappropriate advertising is both fair and reasonable and in the best interests of the child. AANA believes that restricting these practices will lead to consumer harm. AANA is seeking specific clarity on this issue to ensure that advertising of such products can continue to be done in a responsible manner in compliance with the advertising industry self-regulatory Codes.
- The Privacy by Default proposal may have the unintended consequence of depriving the various advertising platforms of the relevant data (e.g. that someone may be a child) which enable appropriate exclusion from certain advertising. Data collection and processing is necessary to ensure a safe online environment and the collection and use of data to ensure online safety from inappropriate content or advertising being served to children or vulnerable groups is something that needs to be balanced with the goal of protecting privacy.

AANA believes the GDPR's 'legitimate interests' test should be introduced as a lawful basis for processing data.

AANA welcomes the proposal for more detailed guidance and standardised templates to assist and promote compliance with the new privacy requirements. AANA believes such templates and

[1] *Advertising Pays: the economic, employment and business value of advertising,* June 2016 http://www.advertisingpays.com.au/

guidance should be in place at least six months prior to the new Privacy Act taking effect to provide businesses with sufficient time to review and adapt systems and ensure they are compliant for the new regime.

AANA would also like to see the government provide more assistance in the area of cyber-security, prevention of data loss and recovery of stolen data. Hacking attempts are likely to increase and become more sophisticated in line with the increased pecuniary penalties and the right to sue which in turn make it more likely that businesses will pay a ransom to retrieve stolen data to mitigate damage to customers. For this reason, it is vital that the Australian government provides more technical and policing resources to prevent cyber-attacks, track down hackers and retrieve stolen data.

Submission

• Proposal 3 – Object of the Act

AANA supports the proposals to clarify the importance of protecting personal information and recognise the public interest in protecting privacy.

• Proposal 4 - Personal information, de-identification and sensitive information

The proposed amendment to the definition of personal information may capture inferred or modelled behaviour that does not currently fall within the definition of personal information. Marketers use such information to build a marketing plan to either include or exclude such consumers from their marketing campaign.

AANA supports the proposals for non-exhaustive lists, case examples and explanatory materials as to what may fall within the definition of 'personal information' and what would be considered 'reasonably identifiable' to provide more clarity around the use of data on inferred or modelled behaviour.

In terms of the proposals for de-identified data, the advertising industry has been moving away from purchasing 2nd and 3rd party data to growing their own 1st party data and this proposal will speed up that process given the logistical complexities and potential liability for failing to ensure erasure and correction of data obtained from another party or provided to another party.

As detailed in previous submissions, such restrictions confer competitive advantage to those established companies with detailed 1st party data to the detriment of new entrants with no existing customer base or 1st party data. The competition impacts of the proposed new privacy regime will be felt over time as established companies with detailed customer databases exercise their marketing advantage over new entrants and small businesses with limited marketing capability.

Although the discussion paper recognises the compliance costs of requiring small business to comply with the proposed new privacy regime, the competition impacts of imposing the complexity and compliance costs onto small business has not yet been fully considered. It is likely that the complexity and compliance costs will represent a significant barrier to entry and benefit established businesses.

• Proposal 10 – Privacy policies and collection notices

AANA supports the proposal for sector-specific standardised templates and layouts, including terminology and icons, for privacy policies and collection notices which we believe will assist both consumers and business.

There appears to be conflict between Proposal 10's requirement that collection notices be 'concise' and the extensive and complex information which must be contained in such notices, including details of disclosure to overseas recipients as set out in Proposal 23.

As such, sector-specific standardised templates and layouts dealing with such issues are required to provide entities with sufficient guidance in order to be compliant with the requirement to provide complex information in a concise manner.

• Proposal 11 – Consent and privacy default settings

Privacy By Default

AANA has concerns regarding the online Privacy By Default proposal set out on Proposal 11.4. This change will have wide sweeping impact on how advertisers can engage with an audience and AANA believes this will result in a sub-optimal and less safe user experience.

The ability to exclude children and other vulnerable groups from seeing advertising for alcohol, gambling and occasional food or drinks is based on behavioural data. For example, even if a child purports to be a certain age to access an app, platforms use age verification technology to compare online behaviour with a user's purported age (e.g. announcing their 10th birthday when they purport to be 13 years of age). Such tools are then used to block access to an app or ensure that inappropriate advertising is not served to that child. Likewise with alcohol advertising, brands can currently use behavioural data to exclude groups of people who are buying maternity wear or pregnancy books. By using this targeting data to exclude certain groups from seeing potentially inappropriate advertising, the online experience is made more safe. By restricting the collection of such data via a Privacy by Default setting, the unintended consequence may be children and other vulnerable people seeing more alcohol, gambling, credit card and occasional food or drink advertising.

AANA believes that overall, the Privacy by Default proposal will lead to a sub-optimal online customer experience which will not meet community expectations. The OAIC Community Attitudes to Privacy 2020 research showed that around 50% of respondents of all ages agreed with the statement "If I have to receive ads, I'd prefer them to be targeted and relevant to me". The proposal will essentially require consumers to opt-in to behavioural advertising (advertising based on user interests) and, assuming few do, will force the move to contextual advertising (advertising based on the content of the page on which the ad appears).

If the Privacy By Default proposal is adopted, further guidance is required on whether measuring the delivery of advertising for audit purposes would be considered fair and reasonable under the new Privacy Act. Following on from the ACCC's Ad Tech Inquiry, the digital advertising industry is currently seeking to implement technical solutions to ensure that advertisers can trace and audit the delivery and effectiveness of online advertising they have purchased via the digital advertising supply chain.

Companies also use data analytics software to gain a better understanding of how the company's website is being used by customers. Data analytics allow website owners to understand which web pages people are visiting, which can in turn be used to create a better user experience for website visitors. It is likely that such data collection will be subject to consent requirements under this proposal for Privacy By Default which will lead to sub-optimal customer experiences online.

Data collection is also used to prevent criminals and other bad actors from profiting from digital advertising. This includes identifying suspicious activity which could signal ad fraud and preventing ads from appearing next to harmful content. Efforts to defund harmful online content by ensuring advertising does not appear near such content should not be unduly hampered by data collection restrictions. As such, if this Privacy By Default proposal is adopted, further guidance is required on how these activities to identify and defund harmful content can continue.

Advertisers also need tools to measure the effectiveness of online advertising. This includes aggregated data used to enable advertisers to know how their ads are performing across different platforms (e.g. how many times it was viewed, for how long etc) and web analytics. Further guidance on this issue would be helpful to determine how this can continue if the Privacy By Default proposal is adopted.

Consent Required to be Current

AANA requests further guidance and sector specific examples of how the currency of consent is to be determined. This guidance would also assist entities when undertaking their analysis for the purposes of setting maximum retention periods as set out in Proposal 21.7.

Legitimate Interests Test

AANA supports the introduction of the GDPR 'legitimate interests' test as a legal basis for processing data in Australia and alternative to obtaining consent. This would allow specific types of data to be used to identify and prevent fraud, ensure network and information security and enable entities to use data in ways that are lawful, proportionate and in the interests of the user.

AANA believes this test is a sensible way to allow entities to use data in ways consistent with customer expectations where explicit consent has not been obtained.

There may be instances where an entity needs to process customer data however explicit consent has not been obtained for that purpose. Under the proposed new rules, it may not be possible for the entity to undertake activities such as fraud prevention or security processes if they have not obtained explicit consent for such uses. A legitimate interest test provides entities with a default mechanism to ensure they can use data in ways that are consistent and in the interests of the user.

• Proposal 12 – Fair and reasonable personal information handling

The definition of 'fair' is not sufficiently defined in the proposal so as to provide entities with guidance as to how this would be implemented. Although the term 'unfair' has precedent and legal meaning, the term 'fair' does not. AANA believes this proposal requires further work and guidance.

If this proposal is adopted, AANA believes that the collection and use of data to exclude children and vulnerable groups from seeing certain advertising is fair and reasonable and in the best interests of the child and requests the OAIC to provide guidance on this issue as a matter of urgency. It is vital for both online safety and brand safety for advertisers to have control over where their advertising appears and access to behavioural data is the best and most accurate method for ensuring this is done in a responsible manner when advertising online.

The advertising self-regulatory system requires advertisers not to advertise alcohol or gambling to minors (under 18 years of age) and not to advertise occasional food (e.g. chocolate) or drinks (e.g. soft drink) to anyone under 15 years of age. The advertising self-regulatory system applies to all advertising, including digital advertising and requires advertisers to ensure they comply with the age

restrictions when placing advertising online by using various targeting tools to include and exclude certain groups from seeing the ad.

The advertising self-regulatory system ensures that advertising is done in a responsible manner, in line with community expectations. AANA requests urgent clarification and guidance from the government to determine whether or not such responsible advertising can take place once the new Privacy Laws take effect.

• Proposal 16 – Children

As stated above, AANA is seeking urgent clarification and guidance as to whether the collection of behavioural data to determine if an online user is a child and then using that data for the purposes of excluding that user from seeing inappropriate advertising (such as alcohol, gambling, credit cards and occasional food or drinks) is fair and reasonable and in the best interests of the child.

• Proposal 17 – People experiencing vulnerability

AANA supports a safe online environment for children and vulnerable people. This issue highlights the conflict between online safety and privacy. AANA is seeking urgent clarification and guidance as to whether the collection of behavioural data which indicates a person may be vulnerable and then using that data for the purposes of excluding that user from seeing inappropriate advertising (such as not showing credit card or gambling advertisements to someone who may be experiencing financial distress) is fair and reasonable.

• Proposal 20 – Direct Marketing, Targeting and Trading

Targeting

AANA is concerned that the proposal to broaden the definition of 'targeting' to cover any information which relates to an individual including deidentified information and unidenitifed information (internet history/tracking etc) would have wide reaching impact on the advertising industry by essentially shutting down targeted marketing, preventing the exclusion of children and vulnerable people from seeing inappropriate advertising (e.g. credit cards, alcohol, occasional food) and resulting in consumers seeing ads that are of no relevance to them.

The tone of the debate on targeted advertising seems to be around it being a behaviour which potentially exploits consumer's vulnerabilities however what is not reflected in the paper is the importance of behavioural data to identify certain groups to ensure they do not see certain advertising. It is not clear from the proposal how exclusion targeting to protect children and vulnerable people would continue to work.

AANA believes providing an opt-out right would raise the cost and lower the effectiveness of advertising as advertising becomes random, irrelevant and fails to engage with consumers. This will be to the detriment of small business, charities and NGOs as personalisation makes advertising relevant to the user and therefore more effective and helps businesses find customers and grow their business. Deloitte's *Dynamic Markets Report* found 71% of Australian small businesses using personalised advertising reported it is important for the success of their business.[2] Similarly, charities

[2] Deloitte, 'Dynamic Markets Report: Australia - unlocking small business innovation and growth through the personalised economy', *Meta Australia blog,* October 2021, https://australia.fb.com/economic-empowerment/

use personalisation to break through 'compassion fatigue', to determine the social causes with which users are most aligned to maximise the likelihood a person will donate to that charity.[3]

The ability of the government to reach target audiences will also be compromised as the data used to determine a particular segment of the population will be unavailable. For example, reaching CALD and First Nation communities will become more difficult if this proposal is adopted.

In addition, AANA believes that the proposals around targeted advertising ignore the importance of advertising to the overall economy and in funding online content and journalism. The economic benefit of the digital advertising ecosystem is summarised as follows in the report *Ad'ing Value: The Impact of Digital Advertising on the Australian Economy and Society* by PWC on behalf of IAB Australia[4]:

Journalism and free online services are reliant on advertising revenue to survive. The majority of consumers recognise that they see advertising as part of the value exchange for free online content. If consumers have to see advertising, research shows that consumers prefer relevant ads according to a report conducted by Infogroup which found that around 90% of people said that messages from companies that are not personally relevant to them are "annoying".[5]

The proposal to allow online users the unqualified right to opt out of their personal information being used for targeted marketing may have the unintended consequence of rendering platforms and advertisers blind as to who will see their ads. Rather than risk children being served with inappropriate ads, advertisers of certain products may opt out of advertising on certain online platforms for brand safety reasons.

In relation to the right to opt out of targeted advertising, it is not clear what 'advertising' would cover. For example, a bank may communicate to their existing customers via a message containing a combination of marketing and service messages, such as messages promoting features of services/products which can help prevent customers becoming victims fraud or scams. Would such communications be categorised as advertising? Being able to distinguish between advertisements and other forms of communication is difficult, particularly for small businesses without significant

[3] C Green, 'What the next generation of personalisation means for charity marketing', *Charity Digital*, 19 August 2020, https://charitydigital.org.uk/topics/topics/what-the-next-generation-of-personalisation-means-for-charity-marketing-7831

[4] *Ad'ing value: The impact of digital advertising on the Australian economy and society*, IAB Australia, November 2022, page 3

[5] Infogroup, *The Power of Personalization*, May 2019, https://www.emarketer.com/chart/228797/attitudes-toward-personalization-among-us-internet-users-jan-2019-of-respondents

marketing, communications and legal resources. AANA believes further guidance is required around the definition of 'advertising' and what would be captured by opting-out.

As outlined above, AANA believes that wholesale restrictions on targeted advertising will have economic and consumer impacts which we believe are harmful and not justified in the name of privacy. AANA welcomes further discussion on this Proposal to ensure that consumer detriment and an unsafe online environment is not an unintended consequence of the new Privacy Act.

Case Study 1 – Hamburger & Chips Advertisement

Under the AANA Food & Beverages Advertising Code, any advertisement for a food or beverage that does not meet the Food Standards Code nutrient profile score criterion (NPSC) must not target children under 15 years of age. As such, an ad for a hamburger and chips product that does not meet the NPSC must not target children. This includes online ads.

When it comes to online advertising for such a product, to ensure compliance, the advertisers for such a product would currently only advertise on online platforms that have age enabled targeting options. They would then specifically exclude contextual placements near content popular with children (e.g. Peppa Pig, Disney shows) and target only content with audiences that are known to be over 18 years of age. Keywords could also be used to include and exclude certain segments to better ensure the advertisement is seen by the target audience.

If the above behavioural data is not available to ensure compliant placement of the ad, more explicit personal data regarding the age of the individual will be required to ensure such advertising is not served to children.

Case Study 2 – Opting Out of Targeted Advertising

Under the proposed new privacy proposals relating to targeting, if a Chrome user opts to not allow targeted advertising, then advertising to that person will not relate to any data points collected regarding that person. If Google knows that user who has opted out is under 15 years of age, under the new regime, that data potentially cannot be shared with the advertiser. This places the advertiser in the situation of not being in control of who will see their advertisement. Brands have Code compliance and brand safety reasons for wanting control over where their advertising appears however brands will in the future be completely dependent on platforms to proactively block users from seeing inappropriate ads rather than having the tools to do so themselves.

Case Study 3 – Technical Challenges of Opting Out

In some cases, an entity may only have deidentified data or some other data points relating to a user – no known customer. Honouring opt out requests is often tied to an email address or phone number of a user or customer. In the case where an unknown user opts out from receiving targeted advertising, honouring that request will prove technically difficult because the entity has no concrete information to which the opt out request can be tied. There is no way to administratively process that request and prevent that user receiving targeted advertising in future because the entity cannot identify the user in the first place.

If the opt-out request is tied to a cookie (even 1st party) the opt-out could be deleted when the user clears their cookies. Advertisers would need the advertising platforms (e.g. Google & Meta) to pass along opt-outs which is currently not done and the feasibility of which is unclear.

Trading

Further clarification is required on the proposed definition of trading information and its application to loyalty programs. Loyalty programs operate by the trading of data and their value to organisations and customers is significantly diminished if data cannot be traded. In relation to a credit card loyalty program, there could be several organisations involved in sharing personal information. For example, the following parties could be involved in sharing data as part of a credit card loyalty program:

- Card issuer (e.g. NAB)
- Payment processor (e.g. Visa)
- Brand owner/partner (e.g. Qantas card, Coles card)
- Cashback rewards programs (either cashback provider or retailer)
- Additional loyalty programs linked to card
- Augmented data brokers

Additional guidance is required to understand what steps would need to be taken for the ongoing operation of these loyalty programs under the proposed new Privacy rules.

• Proposal 21 – Security, retention and destruction

Retention Periods

As stated above, AANA requests further clarification of how to determine the currency of consent. Currency of consent will be a relevant factor when determining maximum and minimum retention periods as required under Proposal 21.7.

The requirement to destroy information will also result in customers having to re-supply information they have previously provided but which has subsequently been destroyed for privacy reasons. This will inevitably lead to customer frustration that they are being forced to provide information and go through processes they had thought they had already completed.

Review of Laws Requiring Retention

AANA supports the proposed review of laws requiring the retention of personal information. Apart from the cyber-security laws, attention should also be paid to State and Territory competitions/contest laws, some of which require the personal details of winners to be published. For example, in South Australia, the initial of the first name, last name and the postcode of each winner must be published within 30 days of the draw.

• Proposal 23 – Overseas data flows

AANA requests guidance and clarification on Proposal 23 in relation to how these requirements would apply to overseas data flows involving multi-national companies where the data is stored within the global corporate entity but in another country in secure data centres as part of a data protection and back-up strategy. For example, a global company's local transaction data may be stored in each local country while customer loyalty program data may be stored in a global database in another country and backed up to another database in another location. Further guidance on how the new proposals would interact with cross-border data transfers within a global corporate entity would be helpful to ensure compliance with this requirement.

Further Consultation

The AANA would welcome an opportunity to discuss in more detail the issues raised in this submission. Please contact Megan McEwin at megan@aana.com.au regarding opportunities for further consultation.