Submission to the Government response to the Privacy Act Review Report

March 2023

Foundation for Alcohol Research & Education

About FARE

The Foundation for Alcohol Research and Education (FARE) is the leading not-for-profit organisation working towards an Australia free from alcohol harms.

We approach this through developing evidence-informed policy, enabling people-powered advocacy and delivering health promotion programs.

Working with local communities, values-aligned organisations, health professionals and researchers across the country, we strive to improve the health and wellbeing of everyone in Australia.

To learn more about us and our work visit www.fare.org.au.

You can get in touch via email at info@fare.org.au

FARE is a registered charity, and every dollar you give helps fund projects keeping our communities healthy and safe. You can make a tax-deductible donation at: www.fare.org.au/donate.

Contents

Executive summary

Everyone should be able to enjoy the benefits of using digital technologies to work, learn and play. This can happen when we have safe digital environments that enable people's health and wellbeing. However, the extensive collection, use and disclosure of people's information is being used to fuel digital marketing practices that are harming our community.

Our key focus in the discussion of privacy reforms is the extensive processing of people's information to relentlessly track, monitor and profile them to target them with advertising tuned to their personal attributes and behaviours to sell them alcoholic products.

Alcohol is an addictive substance that causes significant harm to Australians. Every year, almost 6,000 lives are lost and more than 144,000 people are hospitalised from the use of alcoholic products.[1] Alcohol use causes over 200 disease and injury conditions,[2] contributing to 4.5% of the total burden of disease, [3] and costing Australia an estimated $66.8 billion annually.[4]

Research shows that exposure to online marketing for alcohol is associated with increased use of alcoholic products. Children's exposure to alcoholic product marketing increases the likelihood that they will start drinking earlier and drink at risky levels.[5] A review of research with people experiencing problems with alcohol suggests that the more a person uses alcohol, the more attentive they are to cues like marketing, which in turn leads to increased cravings for alcohol.[6]

The current extensive collection, use and disclosure of people's information enables companies to extensively profile and track people, developing intimate insights into their lives, to increase profit from digital advertising. This commercial cyberstalking enables advertisers to learn people's individual susceptibilities and vulnerabilities to target them with advertising that is most likely to influence their perceptions and behaviour. These insights are used by companies selling addictive and harmful products such as alcohol, to aggressively market their products.[7-9]

Companies selling harmful and addictive products are also increasingly investing directly in the extensive data processing to personalise marketing. For example, in 2022 alone, the alcohol and gambling corporation Endeavour Group invested $35million into their AI-powered personalised marketing engine which is fuelled by data collected on 6.2 million Australians through their My Dans program alone and is trained to find and target people who are most likely to buy alcoholic products.[10-12]

By design, people who purchase harmful and addictive products the most are targeted by digital marketing models the most.[8, 13, 14] Extensive data collection allows digital platforms to develop detailed psychometric profiles that are combined with detailed accounts of people's browsing behaviour.[15] These insights are used to tailor marketing activities, including content and messaging, towards an individual's specific susceptibilities.[15] In the case of alcohol marketing, this ability to prey on people's susceptibilities is particularly harmful because it can disproportionately target people who are at risk of or experience alcohol dependence.[16] FARE and VicHealth conducted a survey of 220 people seeking to reduce alcohol, gambling and unhealthy foods. People who were trying to avoid alcohol advertisements indicated that they were unable to avoid these online, even when they had opted out of marketing;[17]

> *"I am an alcoholic and I feel targeted with marketing that promotes alcohol despite choosing preferences within browsers not to see alcohol." – FARE survey participant*

> *"I struggle with alcohol and have struggled with gambling in the past so when I see [online advertisements], I sometimes get tempted and triggered...The constant bombardment with the marketing is wearing down my resilience." – FARE survey participant*

"I'm in recovery so don't need or want to be seeing alcohol ads." – FARE survey participant

The below-the-line and ephemeral nature of digital marketing also means that companies selling harmful and addictive products can target their digital marketing to children and young people out of sight. For example, companies selling alcoholic products have been shown to upload information about children to digital platforms and for digital platforms to generate and tag children with alcohol-related advertising interests.[18]

A privacy-by-design approach is needed. Being commercially cyberstalked should not be the default requirement for using online services. The health and wellbeing of our families and communities must be prioritised over commercial interests.

Summary of recommendations to the consultation

We welcome the opportunity to provide a submission to the consultation on the Government response to the Privacy Act Review Report (hereafter referred to as the 'Act' and the 'Report').

We support many of the recommendations within the Report. We identify the below key priority areas that to be addressed to reduce harms from data-driven marketing practices.

Update the definition of 'personal information': The definition of personal information is an integral foundation to the protections offered by the Act and must address information used to fuel digital marketing practices. This should specifically include technical, inferred or generated information, and other techniques that relate to a person and can distinguish a person from a group, even if their identity is not known.

Implement a 'fair and reasonable' requirement for data processing: Companies that process people's information should be required to minimise and mitigate harm. A fair and reasonable requirement will introduce minimum standards to hold companies accountable for their data processing activities. This should ensure that risk of adverse impact or harm and the best interests of the child are minimal requirements to be considered in the processing of people's information and these must not be offset by commercial benefits.

Ensure meaningful consent: Strengthened consent mechanisms are important for enabling people to have agency and control over the way their information is processed. Companies should not be able to force, trick or manipulate people into giving consent or rely on the notion of 'implied' consent. Consent must be voluntary, informed, current, specific and unambiguous and indicated through clear action. This must ensure that consent is facilitated through pro-privacy default options (i.e., a person must opt-in rather than opt-out), unbundled consent options (i.e., a person must explicitly opt-in for their data to be processed for marketing purposes, this cannot be captured under a forced 'agree to all' setting), and the provision that data processing must not be made a term or condition for accessing goods or services (i.e., a person should not be forced to agree to have their information processed for marketing purposes in order to access websites, platforms, apps, or other goods or services).

Restrict harmful marketing practices: The extensive processing of people's information contributes to harmful data-driven marketing practices which can exploit people's predispositions and susceptibilities and means that people most at risk of harm are targeted the most. Protections must be implemented for the processing of people's data for all marketing practices, including the collection, use and disclosure of people's information for profiling, targeting and trading. We recommend that:

- The collection, use and disclosure of people's information for all commercial marketing purposes (i.e., marketing, profiling, targeting and trading) require active, informed, voluntary and non-incentivised opt-in consent,

- Even when consent is provided for the collection, use or disclosure of a person's information for marketing purposes:
    - The collection, use and disclosure of sensitive information, which should extend to indicators of a person's use of alcohol or whether they have accessed support for their alcohol use is prohibited, and
    - The collection, use and disclosure of a person's information for all marketing purposes should be required to meet the fair and reasonable requirement whereby it is ensured that the risk of adverse impact and harm are minimised,
- The tracking, profiling, monitoring or targeting of children for commercial purposes be prohibited, and
- The collection, use and disclosure of children's personal information for commercial marketing purposes be prohibited, particularly by, or for, companies selling or marketing addictive or harmful products, including alcohol, gambling, tobacco (including e-cigarettes/vapes), and unhealthy food.

We make further recommendations specific to the proposals as below.

#	Proposal (in brief)	Recommendation
Personal information, de-identification and sensitive information		
4.1	Change 'about' to 'relates to' and include guidance	We support this proposal.
4.2	Non-exhaustive list of examples of personal information	We support this proposal.
4.3	Definition of 'collect' to include inferred and generated information	We support this proposal.
4.4	Definition of reasonably identifiable	We strongly recommend that the definition of reasonably identifiable should include where an individual is distinguished as an individual, even if their identity is not known.
4.6	Apply some APPs to de-identified data	We support that protections in the Act be extended to de-identified information used in profiling activities. However, this may not be necessary if the definition of reasonably identifiable is amended per our recommendation to proposal 4.4.
4.9	Sensitive information	FARE supports this proposal. We recommend that indicators of a person's use of alcohol should be considered sensitive information and that the definition of biometric information is expanded by removing 'that is to be used for the purpose of automated biometric verification or biometric identification.'
4.10	Geolocation tracking data	We recommend that geolocation data should be included in the definition of sensitive data.
Flexibility of the APPs		
5.1	Information Commissioner powers to create an APP code	We support this proposal. The Information Commissioner should be able to make an APP code when it is in the public interest regardless of whether there is an appropriate industry representative to develop the code.

Privacy policies and collection notices		
10.1	Clear and concise collection notices	We support this proposal.
10.3	Standardised notices	We support this proposal. We recommend that notices be developed by the Information Commissioner.
Consent and privacy default settings		
11.1	Definition of consent	We support this proposal. We recommend that 'unambiguous' be changed to 'unambiguous indication through clear action' and that it be assured that consent cannot be tied to the provision of goods and services.
11.2	Consent request design	We support this proposal. We recommend that consent requests be developed by the Information Commissioner.
11.3	Withdrawal of consent	We support this proposal.
11.4	Privacy settings reflect privacy by default framework of the Act	We support the intention that online privacy settings should reflect the privacy by design intent of the Act. We recommend that pro-privacy settings are enabled by default.
Fair and reasonable personal information handling		
12.1	Fair and reasonable requirement	We support this proposal.
12.2	Fair and reasonable requirement considerations	We support this proposal. We recommend that addressing 'the risk of unjustified adverse impact or harm' and 'the best interests of the child' must be minimal requirements that are not offset by commercial benefits.
12.3	Fair and reasonable requirement to apply regardless of consent	We support this proposal.
Additional protections		
13.1	Privacy Impact Assessment for high-risk activities	We support this proposal. We recommend that all businesses are captured within this requirement.
13.2	Enhanced risk assessments for facial recognition technology	We support this proposal.
13.3	Practice-specific guidance for new technologies and emerging risks	We support this proposal.
13.4	Third party collection requirements	We support this proposal.
Children		
16.1	Define a child as <18 years of age	We support this proposal.
16.4	Best interest of the child	We support this proposal.

16.5	Children's Online Privacy Code	We generally support this proposal. We recommend implementation must take a privacy preserving and harm minimisation approach.
People experiencing vulnerability		
17.1	OAIC guidance on vulnerability	We generally support this proposal. We recommend implementation must take a privacy preserving and harm minimisation approach.
Rights of the Individual		
18.1	Access and explanation	We support this proposal. We do not support a fee for access.
18.2	Objection	We support this proposal.
18.3	Erasure	We support this proposal.
18.6	Exceptions	We recommend providing an exhaustive and definitive list of instances where technical impossibilities would be accepted.
Direct marketing, targeting and trading		
20.1	Definitions of direct marketing, targeting, trading	We support the inclusion of clear definitions for marketing, targeting and trading. We provide comments on amending the definitions provided.
20.2	Unqualified right to opt-out of information used or disclosed for direct marketing	We recommend that this unqualified right be extended to the collection, use and disclosure of a person's information for all marketing purposes. We recommend pro-privacy default opt-in requirements for the collection, use and disclosure of a person's information, especially for marketing purposes.
20.3	Unqualified right to opt-out of receiving targeted advertising	We recommend unqualified pro-privacy default opt-in requirements for receiving targeted advertising. We note that this proposal must be implemented alongside proposal 20.2 (with our recommendations under that proposal) so that the collection and disclosure of information for targeting is also addressed.
20.4	Consent requirement for trading	We recommend that this must be unqualified; consent must not be made a term or requirement for accessing goods and services.
20.5	Prohibit direct marketing to children	We support this proposal.
20.6	Prohibit targeting to children	We support this proposal.
20.7	Prohibit trading in the personal information of children	We support this proposal.
20.8	Targeting to be fair and reasonable and prohibit targeting based on sensitive information	We support this proposal. We recommend that this be extended to the collection, use and disclosure of people's information for all marketing purposes.
20.9	Provide targeting information	We support this proposal.

Response to proposals

Our submission is focused on the role that privacy law plays in protecting people from harmful marketing practices, particularly online and focuses on the proposals raised in the Privacy Act Review Report that relate directly to this.

Personal information, de-identification and sensitive information

We strongly support broadening the scope of information regulated under the Act, particularly the inclusion of technical and inferred information which are commonly collected and used for digital marketing practices.

Extensive information is collected about people to fuel data-driven digital marketing practices and extends well beyond information actively provided by people when using online platforms.[8, 19, 20] When it comes to the promotion and sale of harmful and addictive products, these data-driven and highly invasive marketing practices cause harm to the community.

In the case of companies marketing alcoholic products, the extensive collection and analysis of information about people enables alcohol companies to deliver highly personalised digital marketing campaigns that target specific demographics and behavioural profiles, including high frequency of alcohol use. Information from digital platforms, an alcohol company's website and loyalty programs are connected to generate 'custom' audiences made up of the alcohol company's existing customers, and then develop 'lookalike' audiences of potential new customers. These people have similar characteristics to the alcohol company's most profitable existing customers (i.e., people who make more frequent purchases or spend large amounts on alcoholic products) and target this audience with alcohol advertisements.[7]

Alcohol companies know that these sophisticated marketing databases result in higher use of alcoholic products than traditional forms of marketing[21] and continue to invest heavily in these marketing methods despite their harms. For example, in 2022 alone, the alcohol and gambling corporation Endeavour Group have developed invested $35million into their EndeavourX initiative, which uses an AI-powered personalised marketing engine to drive increased sale of alcoholic products.[10, 11] Endeavour Group's personalised marketing engine is fuelled by information about individuals, including data collected on 6.2 million Australians through their My Dans program alone,[12] and is trained to find and target people who are most likely to click through an advertisement to buy alcoholic products.[11] Endeavour Group have described their digital marketing method as the 'Netflix approach' whereby they collect extensive personal information to target individuals with personalised marketing – continually encouraging them to buy more alcohol.[16]

Proposal 4.1 Change the word 'about' in the definition of personal information to 'relates to'.

We strongly support this proposal as it more accurately reflects the current nature of data processing for digital marketing purposes. This will clarify that personal information includes technical and inferred information about a person's activities.

Proposal 4.2 Include a non-exhaustive list of information which may be personal information to assist APP entities to identify the types of information which could fall within the definition. Supplement this list with more specific examples in the explanatory materials and OAIC guidance.

We support this proposal and the list included in the Report.

We note that the Discussion paper explicitly stated that the definition of personal information 'would cover circumstances in which an individual is distinguished from others or has a profile associated with a pseudonym or identifier, despite not being named.'

Proposal 4.3 Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.

We strongly support this proposal.

It is important that inferred or generated information be expressly included in the definition of personal information to ensure this is subject to the same protections as any other type of information. This is particularly relevant to protections that apply in relation to the collection, use or disclosure of personal information for marketing purposes, as inferred information is commonly used by online platforms and advertisers to market harmful products to people, including children, on the basis of inferred information. This must capture current practices, such as the creation and use of lookalike audiences for digital marketing purposes.

Proposal 4.4 'Reasonably identifiable' should be supported by a non-exhaustive list of circumstances to which APP entities will be expected to have regard in their assessment.

We support that the definition of reasonably identifiable should be supported by a non-exhaustive list. However, we strongly recommend that the definition of reasonably identifiable should also include where an individual is distinguished as an individual, even if their identity is not known. We support the definition provided by Salinger Privacy of individuation, to capture this practice which should be addressed as reasonably identifiable: 'the ability to disambiguate or "single out" a person in the crowd, such that they could, at an individual level, be tracked, profiled, targeted, contacted, or subject to a decision or action that impacts upon them - even if that individual's "identity" is not known (or knowable)' (p35 of the Report). It is important that the definition of personal information apply to these situations to ensure additional protections in the Act are meaningful, particularly in the context of the digital environment and for digital marketing purposes.

Proposal 4.6 Extend the following protections of the Privacy Act to de-identified information:

Targeting proposals – the proposed regulation of content tailored to individuals should apply to de-identified information to the extent that it is used in that act or practice.

We strongly support that protections in the Privacy Act be extended to de-identified information used in profiling activities. We note that this proposal will likely be unnecessary if the definition of reasonably identifiable is amended to incorporate individuation.

Proposal 4.9 Sensitive Information

(b) Amend the definition of sensitive information to replace the word 'about' with 'relates to' for consistency of terminology within the Act.

(c) Clarify that sensitive information can be inferred from information which is not sensitive information.

We strongly support that the definition of sensitive information be amended to replace the word 'about' with 'relates to' and to clarify that sensitive information can be inferred from data which is not in and of itself classified as sensitive information.

We recommend that the definition of health under sensitive information should explicitly include all information relating to, or indicating, a person's physical, mental or emotional health and wellbeing. This should include information relating to, or indicating, drug and alcohol use or addiction, mood or emotional state. This information is extremely sensitive about a person. Leaked Meta documents show that Meta has gathered psychological insights on almost 2 million children in Australia and New Zealand to sell targeted advertising.[22] This included monitoring children in real-time to identify their current mood, including when

they feel 'overwhelmed' and 'anxious', to sell targeted advertising.[22] It can be reasonably deducted that this information is similarly being collected and inferred for marketing purposes for other audiences.

We also recommend that the definition of biometric information captured under sensitive information be amended to remove 'that is to be used for the purpose of automated biometric verification or biometric identification'. Biometric information is highly sensitive and should be classified as such under the Act.

Proposal 4.10 Recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent. Define 'geolocation tracking data' as personal information which shows an individual's precise geolocation which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time.

We support that the collection, use, disclosure and storage of geolocation data must require consent. However, geolocation data should be included in the definition of sensitive information as it provides extremely intimate and detailed insights into people's lives as it provides a strong indication of people's preferences and behaviours and enables extremely targeted marketing.[8] Therefore, this information is at risk of being used in ways that can create harm and should be incorporated into the definition of sensitive information. Further, the incorporation of 'tracked over time' should be reconsidered given a single collection could impact a person's privacy rights.

Consultation question: Should consent be required for the collection, use, disclosure and storage of other tracking data, such as health data, heart rate and sleeping schedule, in addition to precise geolocation tracking data?

Consent should be required for the collection, use, disclosure and storage of tracking data, especially biometric and health tracking data. This should include data such as heart rate and sleep data, as indicted in the report, as well as data including alcohol use, food consumption, weight, exercise, menstrual and fertility information and information related to mood and emotional state. As submitted above, this information should constitute sensitive information, for example under biometric or health information.

If the approach of separating this information from sensitive information is progressed, this information should be captured in prohibitions for collecting, using or disclosing this information for commercial marketing practices.

Flexibility of the APPs

Proposal 5.1 Amend the Act to give power to the Information Commissioner to make an APP code where the Attorney General has directed or approved that a code should be made:

(a) where it is in the public interest for a code to be developed, and

(b) where there is unlikely to be an appropriate industry representative to develop the code.

In developing an APP code, the Information Commissioner would:

(a) be required to make the APP Code available for public consultation for at least 40 days, and

(b) be able to consult any person he or she considers appropriate and to consider the matters specified in any relevant guidelines at any stage of the code development process.

We strongly support the proposal to amend the Privacy Act to provide the Information Commissioner with additional power to make an APP Code on the direction or approval of the Attorney-General, where it is in the public interest to do so without first having to seek an industry code developer.

We recommend that this proposal be slightly amended so that the Information Commissioner can make the APP code in either circumstance, i.e., either

a) Where it is in the public interest for a code to be developed, OR
b) Where there is unlikely to be an appropriate industry representative to develop the code.

This is important as the two might be in conflict of one another and the Information Commissioner should be able to make an APP Code where it is in the public interest to do so without first having to seek an industry code developer, regardless of whether there is an appropriate industry representative to develop the code. This second limb might act to limit the Information Commissioners ability to develop a code in the public interest in the case of vested corporate conflicts of interest.

If the proposal continues, detail regarding the application of the second limb should make explicit that it should not apply where there is deemed to be vested corporate conflicts of interest that might interfere with the development of a code that acts in the publics best interest.

Privacy policies and collection notices

Notices and privacy policies are an important source of information for people on how companies intend to collect, use and disclose their personal information. However, we note that notice requirements are not sufficient on their own and must be coupled with meaningful consent mechanisms and protections against harmful data processing practices. A privacy by design approach is needed.

We agree that both privacy policies and collection notices are retained given each serves a distinct and important function, as is recommended in the report.

Proposal 10.1 Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise and understandable. Appropriate accessibility measures should also be in place.

We support this proposal.

Proposal 10.3 Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP codes that may apply to particular sectors or personal information-handling practices.

We support this proposal for standardised privacy notices. We strongly recommend that the standardised notices are developed by the Information Commissioner in consultation with consumer and data rights groups, designed to facilitate informed consent and be subject to consumer testing. The process should not be industry-led given the commercial conflicts of interest.

It is also important to consider how notice requirements interact with consent requirements. These two elements may need to be combined in many cases, and the design of standardised notices must be undertaken to ensure people are not incentivised or otherwise encouraged to consent by the way the notice is designed. This is important to enable valid consent, per the definition in proposal 11.1.

Once the standardised notices are developed and validated with consumer testing, these should be introduced as a mandatory requirement.

Consent and online privacy settings

We support a robust definition of consent which enables individuals to have real choice and control over the processing of their information. However, consent should not be relied on alone to shift the burden of

monitoring and assessing entities data handling practices to individuals. To ensure consumers are best supported and potential harms minimised, a privacy by design approach is needed, whereby the entire system is designed in a way that preserves privacy and minimises risk of adverse impacts and harms.

Consent mechanisms should support the broader reforms proposed. Particularly, consents should not be able to override other protections or enable harmful data handling processes. The Act's proposed fair and reasonable requirement and prohibited marketing practices must apply even when consent has been given.

Proposal 11.1 Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.

We strongly support the proposal to amend the definition of consent to provide that it must be voluntary, informed, current, specific and unambiguous. Consent for the collection, use and disclosure of people's information should not be assumed, including through 'implied' consent, as is currently enabled under the Act. We agree with the descriptions of each term outlined in the discussion paper. In particular:

- We strongly support that consent will only be considered **voluntary** where the individual has a clear and genuine option not to provide consent, specifically, that if 'consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given' (as is stated in Guidance related to the GDPR; Report p105). Consent is not voluntary where the provision of a service is conditional on consent to all personal information handling practices – particularly for marketing purposes. This must be made explicit.
- We strongly support the requirement that consent be an **unambiguous** indication through clear action. We agree with the OAIC guidance that notes the 'use of an opt-out mechanism to infer an individual's consent will only be appropriate in limited circumstances, as the individual's intention in failing to opt-out may be ambiguous' (Report p105). The Act must require individuals to actively express a choice, and the only way this can be done is via an opt-in mechanism that clearly separates all consent requirements so that individuals must make an express opt-in choice for each purpose. To ensure that the intent of this part of the definition of consent is clear, we recommend that unambiguous 'indication through clear action' be retained (as per proposal 9.1 in the Discussion Paper).
- We strongly support the requirement that consent be **specific** as to what the consent relates to. Consent is not provided if done so through a bundled or broad consent mechanism. It is also not provided for undefined future uses (per APP guidelines; Report p105). This is also important from a data-minimisation perspective, as data shouldn't be collected just in case it might be useful in some way at a later point in time – entities should have a clear understanding of why they are collecting data and the specific use for that data before collecting the data, and subsequently, individuals should be notified of this and provide consent prior to this information being collected.

We support that further detailed guidance can be provided by OAIC indicating when consent does not meet these criteria, and we agree that this should include acceptance of a general or broad terms of use, hovering over, muting, pausing or closing a given piece of consent, or agreement obtained through use of dark patterns.

It is important that this definition of consent is not undermined in the Act. For this reason, it is important that further consideration is given to pro-privacy default settings which require opt-in unbundled consent. This is especially important when it comes to the collection, use and disclosure of information for marketing purposes. The collection, use and disclosure of information for marketing purposes must not be bundled as a non-negotiable term of condition for accessing a service.

Proposal 11.2 The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent,

and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing standardised consents as part of any future APP codes.

We support that the OAIC develop guidance on how online services design consent request. We recommend that consideration be given to further progressing standardises consents, and that these should be developed by the Information Commissioner in consultation with consumer and data rights groups, and be subject to consumer testing. Consent requests should be designed to facilitate voluntary informed consent, considering the elements of consent discussed above.

It is also important to consider how consent requirements interact with notice requirements. These two elements may need to be combined in many cases, and the design of standardised consent must be undertaken to ensure people are not incentivised or otherwise encouraged to consent by the way the consent mechanism is designed.

Proposal 11.3 Expressly recognise the ability to withdraw consent, and to do so in a manner as easily as the provision of consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

We support that an individual should be able to withdraw their consent at any time and to be able to do so as easily as providing consent.

Proposal 11.4 Online privacy settings should reflect the privacy by default framework of the Act.

We support the intention that online privacy settings should reflect the privacy by design intent of the Act. However, we are concerned that in its current form, the proposal will not achieve what it sets out to do. We suggest that Option 1 presented in the Discussion Paper on this proposal, that is, pro-privacy settings enabled by default, remains a more appropriate solution to address privacy by design. Option 1 set out that where an entity offers a product or service that that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. We strongly support this approach.

The Report suggests that the combination of existing mechanisms in the Act and the proposed fair and reasonable requirement will 'effectively operate as a requirement similar to Option 1 and give effect to the data minimisation principles underpinning the Act' (Report p108). While the proposed fair and reasonable requirement and other select proposals in the Report are highly important for contributing to the higher principles of the Act, we do not believe that they operate similar to Option 1 on pro-privacy settings from the Discussion Paper or replace the need for Option 1 on pro-privacy settings.

The evidence presented within the Report indicates that consumers want an opt-in rather than opt-out approach for non-essential uses of personal information (such as marketing; Report p107). This is similarly supported by a nationally representative survey of 1,000 Australians by the Consumer Policy Research Centre conducted in March 2023 which found the vast majority of respondents (88%) expect businesses to protect people against the collection of their personal information, and, to ensure that people are not opted-in by default for the collection, use and disclosure of their data.[23] Additionally, the evidence presented with the Report also indicates that the default option is more likely to be 'chosen' (Report p107 and p108). This calls into question the 'voluntary' and 'unambiguous' nature of this form of 'choice'. Therefore, taking an opt-out approach to the collection, use and disclosure of a person's information both undermines what consumers want and the ability for them to provide valid active consent.

The pro-privacy settings proposed in Option 1 of the Discussion Paper will contribute to data minimisation, a safeguard for children and people experiencing vulnerability, the ability for consumers to provide valid active consent and aligns with what consumers wants.

Fair and reasonable personal information handling

Entities that collect, use or disclose people's information should be required to minimise and mitigate harm. Introducing stronger requirements for how entities handle people's personal information is an important step in shifting the burden of examining and evaluating privacy practices away from individuals and giving companies responsibility to ensure their data handling practices are fair and reasonable. This shift is entirely appropriate and necessary, particularly in the current digital environment.

Proposal 12.1 Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person.

We strongly support this proposal.

Proposal 12.2 In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account:

(a) whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances

(b) the kind, sensitivity and amount of personal information being collected, used or disclosed

(c) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency

(d) the risk of unjustified adverse impact or harm

(e) whether the impact on privacy is proportionate to the benefit

(f) if the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child, and

(g) the objects of the Act.

We support the inclusion of the proposed legislated factors relevant to consider in determining whether data processing activities are fair and reasonable. We recommend that entities are required to satisfy each factor for their data processing activities to be considered fair and reasonable, rather than general considerations that are balanced. At the very least, the factors addressing 'the risk of unjustified adverse impact or harm' and 'the best interests of the child' must be minimal requirements that are not offset by commercial benefits. If an entity is not able to conclude that the collection, use and disclosure of data will not cause harm and is in the best interests of the child, they should not proceed with the collection, use or disclosure of a person's information.

The risk of unjustified adverse impact or harm: We strongly support the requirement to ensure that data processing activities do not pose a risk of adverse impact or harm when considering what constitutes fair and reasonable. We note that the Discussion Paper clearly articulated that this factor would 'require consideration of potential adverse consequences to either an individual, or society, arising from the processing of personal information' (p87). The Report only notes that this factor would require consideration of harm posed to individuals. We recommend that consideration of collective harm is explicitly captured under this factor.

If the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child: We strongly support this requirement and discuss factors related to this requirement under proposal 16.4.

The kind, sensitivity and amount of personal information being collected, used or disclosed: We strongly support the intention for this factor to introduce a data minimisation approach. We support that 'sensitivity' in this factor is not limited to the scope of the definition of sensitive information in the Act.

Whether the impact on privacy is proportionate to the benefit: While proportionality may be appropriate when considering whether the individual's loss of privacy is proportional to benefits in the public interests, proportionality in the fair and reasonable test must not place the commercial benefits of processing personal information above people's privacy or potential adverse impact or harms. As above, we agree that the impact on both individuals and the collective should be considered.

Whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances: This factor must ensure that companies are not enabled to make biased assessments of what a 'reasonable person' might expect. Any assessment of what an individual would reasonably expect must not reflect the current situation whereby extensive collection, use and disclosure of personal information occurs as a means to dismiss this behaviour as reasonably expected. We agree that a description of how personal information will be handed in an entity's privacy policy is not sufficient to meet this factor in the fair and reasonable requirement.

Whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency: It is not clear how this factor will be assessed where a company's core business model or activities are ground in the collection, use or disclosure of personal information. When considering commercial marketing functions and activities, whether the collection, use or disclosure is deemed to be reasonably necessary to achieve these functions and activities, this must not be placed above or balanced with other factors in the fair and reasonable test.

Individual's vulnerabilities and information relating to this should be treated with a higher degree of care. Under 'protections for people experiencing vulnerability,' the Report suggests that a protection could be added to the fair and reasonable assessment of risk of unjustified adverse impacts or harm that would require consideration of handing information of people experiencing vulnerability, or engaging in activities which could have a significant effect on people experiencing vulnerabilities (Report p159). We recommend that this be incorporated into the fair and reasonable assessment.

Proposal 12.3 The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should apply irrespective of whether consent has been obtained.

We strongly support that the collection, use and disclosure of personal information must be fair and reasonable irrespective of whether consent has been obtained to collect, use or disclose personal information.

Additional protections

Proposal 13.1 APP entities must conduct a Privacy Impact Assessment for activities with high privacy risks.

(a) A Privacy Impact Assessment should be undertaken prior to the commencement of the high-risk activity.

(b) An entity should be required to produce a Privacy Impact Assessment to the OAIC on request.

The Act should provide that a high privacy risk activity is one that is 'likely to have a significant impact on the privacy of individuals'. OAIC guidance should be developed which articulates factors that that may indicate a high privacy risk, and provides examples of activities that will generally require a Privacy Impact Assessment to be completed. Specific high risk practices could also be set out in the Act.

We support this proposal.

We support that Privacy Impact Assessments are requestable by the OAIC as this will assist in creating transparency and accountability. We recommend that this provision go further, by requiring Privacy Impact Assessments be publicly available to increase transparency and accountability to the public whose data may be used in a restrictive practice. This will also enable civil society to assess potential high-risk activities and raise any potential further harms that may not be assessed. Making these available in an OAIC-approved standardised format will assist policymakers, civil society and the public in their ability to easily assess and understand Privacy Impact Assessments.

We support that a non-exhaustive list for high-risk practices and recommend that this includes the collection, use or disclosure of data for tracking, profiling and targeting purposes including for targeted/personalised advertising and content.

Proposal 13.2 Consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require Privacy Impact Assessments for high privacy risk activities. This work should be done as part of a broader consideration by government of the regulation of biometric technologies.

We support this proposal.

We have strong concern about the potential use of facial recognition technology, and other biometric information, in alcohol and gambling venues and in alcohol retail outlets. The collection, use and disclosure of biometric information is particularly risky within alcohol and gambling venues and retail outlets because of the addictive nature of alcohol and gaming products, and the fact that these industries rely upon a small cohort of people to generate up to 75 per cent of their profits.[24] These people are likely to be people who are dependent on alcohol and/or gambling.

We are therefore gravely concerned about the following risks of facial recognition technology use in liquor and gaming venues:

- The use of FRT data for marketing purposes, including linking the offline and online behaviours of individuals in order to produce highly personalised advertising. Businesses are promoting facial recognition technology as a way to capture data about people's emotions or to show personalised advertising to patrons.[25] As noted above, we are especially concerned about the targeted advertising of addictive products to individuals who are especially vulnerable to the harms that these products can cause.
- The high probability that alcohol and gambling venues using facial recognition technology will identify individuals in error, leading to those individuals being wrongfully excluded – or even unlawfully arrested or detained. We note that this technology has been found to have the highest rates of error when identifying people of colour, women and people with a disability and thus has a highly discriminatory impact.
- The use of facial recognition technology to exclude, isolate, blame and punish people with dependencies, at the cost of other, more effective and system-wide responses.

Consultation question, proposal 13.2: What additional requirements should apply to mitigate privacy risks relating to the development and use of facial recognition technology and other biometric information?

We recommend that this biometric information is defined as sensitive information and that this should not be collected, used or disclosed for any marketing purposes.

Proposal 13.3 The OAIC should continue to develop practice-specific guidance for new technologies and emerging privacy risks. Practice-specific guidance could outline the OAIC's expectations for compliance with the Act when engaging in specific high-risk practices, including compliance with the fair and reasonable personal information handling test.

We support this proposal.

Proposal 13.4 Include an additional requirement in APP 3.6 to the effect that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3. OAIC guidelines could provide examples of reasonable steps that could be taken.

We support this proposal.

Children

We strongly support that consideration is being given to how to protect children's privacy and rights in online settings. As we discuss under the proposed data processing activities for marketing purposes regarding children, they are currently being extensively tracked, profiled and targeted online. Child-specific protections, such as the prohibitions under the marketing proposals will provide a level of protection for children online. However, creating safe online settings for everyone will have the benefit of protecting children online without increasing practices of age verification that increase privacy risks for children. This includes the implementation of pro-privacy default settings, data minimisation and fair and reasonable requirements that ensure risks of adverse impact and harm are prevented or mitigated and the best interests of the child are met.

Proposal 16.1 Define a child as an individual who has not reached 18 years of age.

We support this proposal.

Proposal 16.4 Require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances.

We strongly support the requirement for organisations to assess whether the collection, use or disclosure of personal information is in the best interest of the child. The commercial interests of an organisation must never outweigh a child's rights to privacy – this should be made explicit.

When it comes to online entities, we agree that entities should be required to consider the best interests of children that may be accessing online services generally in the design of services, and that this should ensure that entities don't embark on intrusive analysis of people's online activities to identify children, their activities, characteristics or circumstances. We agree that this should be clarified in any explanatory material that accompanies reforms (Report p152).

When considering what is in the best interest of the child, it should be explicit that regardless of consent, the following are not considered to be in the best interest of the child and therefore must not meet the fair and reasonable requirement (and should be prohibited practices):

- The profiling, tracking and targeting of children for commercial purpose (as is recommended by the United Nations Committee on the Rights of the Child),[26] and
- The collection, use or disclosure of children's personal information by, or for, companies selling or marketing addictive or harmful products, including alcohol, gambling, tobacco (including e-cigarettes/vapes), and unhealthy food.

We elaborate on this under the prohibitions proposed regarding marketing, targeting and trading.

Proposal 16.5 Introduce a Children's Online Privacy Code that applies to online services that are 'likely to be accessed by children'. To the extent possible, the scope of an Australian children's online privacy code could align with the scope of the UK Age Appropriate Design Code, including its exemptions for certain entities including preventative or counselling services.

The code developer should be required to consult broadly with children, parents, child development experts, child-welfare advocates and industry in developing the Code. The eSafety Commissioner should also be consulted.

The substantive requirements of the Code could address how the best interests of child users should be supported in the design of an online service.

We generally support that the introduction of a Children's Online Privacy Code might help provide protections for children online. However, we are concerned with how the implementation and compliance of such a code may lead to widespread age verification processes that might create additional privacy risks in order to differentiate between children and adults using online platforms and services.

Any requirements to implement child-specific protections must be subject to strong privacy controls and be distinct from identity verification. Measures must take a data minimisation approach (i.e., not permit or require companies to collect and triangulate data to determine if an individual is likely a child) and must mitigate any additional privacy risks. Any attempt to establish a person's age with a high level of certainty will create additional privacy risks. Processes for age verification involving the use of official identity documents, cross-referencing with other databases to check age, or facial recognition technology, all require the collection, use or disclosure of additional personal information and in doing so create disproportionate privacy and digital security risks. We strongly recommend that point 4 under proposal 16.5, i.e., 'whether entities should be required to "establish age with a level of certainty that is appropriate to the risks" or apply the standards in the Children's Code to all users instead' take focus on the latter approach which encourages safer online settings by design.

To ensure that a privacy preserving code that is in the best interests of the child is developed, we strongly recommend that the OAIC should be appointed as the code developer with the intent of the code being mandatory, instead of adopting an industry-led self-regulatory model. It must not be led by industry stakeholders who have commercial conflicts of interest on the matter.

We strongly support the proposal that the code be developed in consultation with children, parents, child development experts and child-welfare advocates and the eSafety Commissioner. We strongly recommend that digital rights advocates and the National Children's Commissioner also be consulted in the development of the code.

People experiencing vulnerability

When it comes to addressing vulnerabilities, a privacy by design approach is important. Under this topic, we reiterate the importance of pro-privacy opt-in default settings, an expansion of information treated as sensitive, and the inclusion of the requirement to reduce risk of adverse impact of harm in the fair and reasonable requirement. These measures will provide important overarching protections for people experiencing vulnerabilities.

Proposal 17.1 Introduce, in OAIC guidance, a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information.

We support this proposal. However, per our comments above regarding identification of children, we strongly recommend that any measure to protect people experiencing vulnerability should be privacy preserving and not enable additional data collection to identify vulnerabilities.

Rights of the Individual

Proposal 18.1 Provide individuals with a right to access, and an explanation about, their personal information if they request it, with the following features:

(a) an APP entity must provide access to the personal information they hold about the individual (this reflects the existing right under the Act)

(b) an APP entity must identify the source of the personal information it has collected indirectly, on request by the individual

(c) an APP entity must provide an explanation or summary of what it has done with the personal information, on request by the individual

(d) the entity may consult with the individual about the format for responding to a request, and the format should reflect the underlying purpose of ensuring the individual is informed, as far as is reasonable, about what is being done with their information

(e) an organisation may charge a 'nominal fee' for providing access and explanation where the organisation has produced a product in response to an individual

We support that people are provided with the right to access their information and an explanation about how their information is being used. We support points a-d under this proposal. However, we do not support that people are charged a fee to access the information an entity holds on them.

Proposal 18.2 Introduce a right to object to the collection, use or disclosure of personal information. An APP entity must provide a written response to an objection with reasons.

We support this proposal.

Proposal 18.3 Introduce a right to erasure with the following features:

(a) An individual may seek to exercise the right to erasure for any of their personal information.

(b) An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort.

We support this proposal.

Proposal 18.6 Introduce relevant exceptions to all rights of the individual based on the following categories:

(a) Competing public interests: such as where complying with a request would be contrary to public interests, including freedom of expression and law enforcement activities.

(b) Relationships with a legal character: such as where complying with the request would be inconsistent with another law or a contract with the individual.

(c) Technical exceptions: such as where it would be technically impossible, or unreasonable, and frivolous or vexatious to comply with the request.

We are concerned that the description of technical expectation under 18.6(c), 'such as where it is technically impossible, or unreasonable, and frivolous or vexatious' are ambiguous and might result in entities finding loopholes to comply with people's rights or creating systems that make it technically impossible to comply with these rights. We recommend providing an exhaustive and definitive list of instances where technical impossibilities would be accepted.

Direct marketing, targeting and trading

We strongly support the implementation of protections around marketing practices, including the collection, use and disclosure of people's information for profiling, targeting and trading.

There are two overarching gaps with the proposals put forward.

Firstly, many of the proposals have not explicitly noted that the *collection* of information for marketing purposes will be captured.

Secondly, we strongly recommend that a privacy-preserving opt-in approach is taken, whereby individuals must first opt-in for their information to be collected, used or disclosed for marketing purposes. This is important to ensure that valid consent is obtained by individuals before collecting, using or disclosing their information for marketing purposes. As outlined in the definition of consent, an opt-out approach is unlikely to constitute valid consent through voluntary and unambiguous action.

Proposal 20.1 Amend the Act to introduce definitions for:

(a) Direct marketing – capture the collection, use or disclosure of personal information to communicate directly with an individual to promote advertising or marketing material.

(b) Targeting – capture the collection, use or disclosure of information which relates to an individual including personal information, deidentified information, and unidentified information (internet history/tracking etc.) for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class).

(c) Trading – capture the disclosure of personal information for a benefit, service or advantage.

We support that direct marketing, targeting and trading will all explicitly be captured within the Act.

Regarding the definitions provided, we make the following comments:

Direct Marketing: We support that the definition clarifies that marketing is not limited to the promotion of goods and services but also the promotion of the aims and ideals of an organisation. We recommend that 'direct' is removed from the definition so that marketing via an intermediary is captured when the marketing is based on a person's information.

Targeting: We strongly support that this captures deidentified and unidentified information, which is often used for targeted marketing. However, we refer to our above comments regarding proposal 4.4 and the definition of reasonably identifiable that individuation should explicitly be covered in the definition of personal information so to include information where an individual may be singled out even if their identity is not known; this would provide more comprehensive consumer protection. We support that the definition expands beyond advertising so not to create difficulty in distinguishing targeted advertising content.

The Report also presents the relationship between profiling, targeting and trading (Report p204). It is important that the act of profiling is addressed in the Act as well as the act of targeting. This is important because the act of profiling, i.e., the act of 'automated processing of personal data consisting of the use of personal data to evaluate certain aspects relating to a natural person...' (as captured under the GDPR)

poses privacy risks and potential harms. It directly relates to people's information being collected and used to build inferences, and therefore this should require people's active consent.

Trading: We recommend that the definition of trading should include the collection and use of personal information as well as its disclosure. Additionally, this protection should extend to information where an individual may be singled out even if their identity is not known. As per our above comment, we recommend that this should be incorporated into the definition of personal information so to provide more comprehensive consumer protection.

Proposals 20.2, 20.3 and 20.4 – Individual rights on direct marketing, targeting and trading.

We strongly recommend that the collection, use and disclosure of people's information for all commercial marketing purposes (i.e., marketing, profiling, targeting and trading) require active, informed, voluntary and non-incentivised opt-in consent. This approach would require that no personal information is collected, used or disclosed for commercial marketing purposes by default, so that consent is never assumed. It is a notable gap in the current proposals (20.2-20.4) that an opt-out rather than a pro-privacy opt-in approach has been taken. Opt-out approaches do not constitute consent, as is presented when defining consent in the Report (which we support).

A survey by FARE and VicHealth conducted with 220 people seeking to reduce alcohol, gambling and unhealthy foods found that over 90% of participants were concerned about online marketing for the products they are trying to reduce and 83% felt that seeing marketing for these products makes it harder for them to reduce their use or consumption of these products.[17] Some participants raised in open-end responses that they continue to receive online marketing for harmful and unhealthy products even after changing online settings, including unsubscribing to mailing lists, in an attempt to avoid this marketing.

> *"I am an alcoholic and I feel targeted with marketing that promotes alcohol despite choosing preferences within browsers not to see alcohol." – Survey participant*

> *"I've restricted ads for alcohol on FB [Facebook], YouTube and Instagram and they still appear." – Survey participant*

> *"I am pretty good at deleting and unsubscribing, but it took me about 4 months of emails to unsubscribe. I am sure I noticed sales on products I have bought before and on one occasion did buy the product. I definitely think more about alcohol when the emails from Dan's [Dan Murphy's] keep popping up. I think for anyone with a history of harmful alcohol use it would be extremely triggering. It's also relentless." – Survey participant*

Opt-in measures must be facilitated by consent mechanisms that are not designed to nudge or coerce individuals to consent to the processing of their personal information for commercial marketing purposes, for example through bundled consents, 'consent to all' options that incorporate marketing consents, or through requiring consent to process data for marketing purposes to access a service.

Additionally, these protections must also extend to the collection of information for marketing purposes (not just the use or disclosure of information).

This is important to address the underlying privacy risks and harms related to these practices.

Once opt-in consent has been provided, individuals should then still have an unqualified right to withdraw their consent (or, 'opt-out') of their information being collected, used or disclosed for any commercial marketing purposes.

We provide further detailed response to each proposal below.

Proposal 20.2 Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes.

Similar to the existing requirements under the Act, entities would still be able to collect personal information for direct marketing without consent, provided it is not sensitive information and the individual has the ability to opt out.

We support that people be provided with an unqualified right to opt-out of their information being collected, used or disclosed for marketing purposes. Therefore, we oppose the part of this proposal which would allow entities to collect a person's information for marketing without their consent.

The Report raises an objection that the collection of information for marketing purposes should not be included in this proposal to accommodate for when a business collects a person's information without knowing at the point of collection that they might use this information for marketing purposes (Report p211). We strongly oppose that this is an appropriate reason to exclude protections around the collection of information as it undermines the privacy-by-design principle of the Act, particularly regarding data minimisation. It also undermines the provision of consent, which should be specific (i.e., 'the intent of an APP entity should not seek a broader consent than is necessary for its purposes, for example, consent for undefined future uses' (Report p105). Therefore, an entities intent of data collection should be known at the point of collection (and be notified and consent provided at point of collection). If an entity later decides they would like to use the information they have already collected for additional purposes, such as marketing, they should be required to receive active valid consent to do so. This would take a data minimisation and privacy preserving approach and reduce risk of harms.

Further, while we support the unqualified right to opt-out, this should not replace a model that is designed to protect privacy, where the default position requires consent to be provided for the collection, use and disclosure of a person's information for marketing purposes. In operation, this would mean that once opt-in consent has been provided for the collection, use and disclosure of a person's information for marketing purposes, an individual would then still have an unqualified right to withdraw their consent (or, opt-out) of their information being collected, used or disclosed for any commercial marketing purposes. It should be clear to entities that they cannot continue to use this information for data processes that underpin the act of delivering marketing.

We strongly support that this will be an unqualified right. Specifically, that not consenting to the collection, use or disclosure of a person's information should not be used to deny a person the ability to access a service.

Lastly, we recommend that this unqualified right be extended to all marketing (i.e., marketing, targeting and profiling). We discuss this further below.

Proposal 20.3 Provide individuals with an unqualified right to opt-out of receiving targeted advertising.

We support that people be provided with an unqualified right to opt-out of receiving targeted advertising. We strongly support that this right is unqualified and that receiving targeted advertising should not be made a requirement to access services. However, we note that this proposal falls very short of addressing the underlying data processing practices which risk privacy and other harms related to targeted advertising. Namely, this proposal does not implement broader protections around the collection, use and disclosure of a person's information for targeting purposes. This may be particularly misleading for individuals, who may opt-out of receiving targeted advertising, but may not understand that their information is still being collected and used for marketing purposes.

We recommend that proposal 20.2 could be extended to include all marketing purposes, noting the additional comments we have made regarding the proposal. In practice, this would mean that the collection, use and disclosure of people's information for all commercial marketing purposes (including profiling, targeting and trading) would require active valid consent. Once opt-in consent has been provided for the collection, use and disclosure of a person's information for marketing purposes, an individual would then still have an unqualified right to withdraw their consent (or, opt-out) of their information being collected, used or disclosed for any commercial marketing purposes (including targeted marketing).

This pro-privacy approach will reduce burden on individuals who largely don't want their information to be used in this way. A nationally representative survey by the Consumer Policy Research Centre of 1,000 Australians in early March 2023 found that less than 10% of people are comfortable with the current approach to targeted advertising with tracking of online behaviour or personal characteristics without giving expressed permission. The vast majority of respondents expected businesses to protect people against the collection of their personal information and to ensure that people are not opted-in by default for the collection, use and disclosure of their data (88% both respectively).

Proposal 20.4 Introduce a requirement that an individual's consent must be obtained to trade their personal information.

We are concerned that this current proposal is limited in scope and may undermine consent. Specifically. We are concerned that this proposal may result in consent being tied to the access of goods and services ('Where consent to trade in personal information was made a condition of accessing goods or services…,' Report p214). This undermines the definition of consent (per proposal 11.1) because it does not constitute voluntary consent.

Additionally, it is important that the scope of information captured under this requirement extends to de-identified and un-identified information. As above, including individuation in the definition of personal information will help address this.

We also note that while this proposal would be an improvement, further consideration should be given to prohibiting the trade in personal information. We support CHOICE and Digital Rights Watch in their position that prohibiting the trade in personal information will reduce the significant risks associated with this practice.

Proposals 20.5, 20.6 and 20.7 – Childrens rights on direct marketing, targeting and trading.

Proposal 20.5 Prohibit direct marketing to a child unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests.

Proposal 20.6 Prohibit targeting to a child, with an exception for targeting that is in the child's best interests.

Proposal 20.7 Prohibit trading in the personal information of children.

We strongly support that the collection, use and disclosure of children's information for commercial marketing purposes be prohibited. To this end, we strongly support proposals 20.5, 20.6 and 20.7.

This is important as research has shown that harmful profiling and targeting of children for commercial marketing purposes is occurring in Australia. This is a particularly significant concern when it comes to the collection, use and disclosure of children's information for the marketing of addictive and harmful products such as alcohol.

Recent research conducted with children and young adults aged 16-25 years old in Australia illustrates that extensive data processing is being used to tune digital marketing models to learn and target young people's predispositions toward the consumption of harmful and addictive products.[18] The research found that the

young participants had an average of 194 advertisers upload data about them to Meta and that the Meta advertising model generated 787 advertising interests about them.[18] This included the Meta advertising model assigning alcohol-related advertising interests, including 41 alcohol-related advertising interests assigned to 5 participants under the age of 18 (e.g., 'alcohol', 'bars', 'beer'). Two alcohol retailers had uploaded data about a participant under the age of 18 years old.[18]

Regarding proposals 20.5, 20.6 and 20.7, we note that our comments above regarding marketing related definitions in proposal 20.1, and the importance of expanding the definition of personal information to include individuation are relevant. We would also like to note that these proposals must be sure to capture each the collection, use and disclosure of a child's information, not solely the act of delivering/targeting marketing materials.

We also submit that when considering what is in the best interest of the child, guidance under the Act should be explicit that the collection, use and disclosure of children's information for any commercial marketing purposes (including tracking, profiling and targeting) by, or for, entities selling or marketing addictive or harmful products, including alcohol, gambling, tobacco (including e-cigarettes/vapes), and unhealthy food, are not considered to be in the best interest of the child and therefore be prohibited.

We also reiterate our comments under proposal 16.4, that entities must not embark on intrusive analysis of people's online activities to identify children, their activities, characteristics or circumstances.

Proposals 20.8 and 20.9 – Additional protections for direct marketing, targeting and trading.

We support that protections are in place to prevent harm from digital marketing practices, even when consent is provided by a person for the collection, use and disclosure of their information for marketing purposes.

Proposal 20.8 Amend the Act to introduce the following requirements:

(a) Targeting individuals should be fair and reasonable in the circumstances.

We support that where not expressly prohibited, the collection, use and disclosure of a person's information for all marketing purposes should be required to meet the fair and reasonable test whereby it is ensured that the risk of adverse impact and harm are minimised. Therefore, we recommend that this proposal be extended to include all marketing practices (e.g., marketing, profiling, tracking and targeting). This must be required regardless of consent to data processing.

(b) Targeting individuals based on sensitive information (which should not extend to targeting based on political opinions, membership of a political association or membership of a trade union), should be prohibited, with an exception for socially beneficial content.

We strongly support that, even when consent is provided for the collection, use and disclosure, of a person's information for commercial marketing purposes, that the collection, use or disclosure of sensitive information for commercial marketing purposes should be prohibited. Therefore, we recommend that this proposal be extended to include all marketing practices (e.g., marketing, profiling, tracking and targeting). This must be required regardless of consent to data processing. Additionally, per our recommendations above, this must apply to each the collection, use and disclosure of sensitive information for marketing purposes, not solely the act of delivering/targeting marketing materials.

We support the intent in this prohibition that this should also extent to sensitive traits, not solely 'sensitive information'. This will be particularly important if proposal 4.10 is progressed by not capturing location and other tracking data as sensitive information. We strongly recommend that indicators of a person's use of

harmful and addictive products like alcohol, or whether they have searched or accessed support for their alcohol use cannot be used to target them with commercial marketing.

Participating in help-seeking activities, such as attending Alcoholics Anonymous meetings and following Alcoholics Anonymous related support pages, were also previously reported to result in receiving increases amounts of alcohol adverts online.[27] This phenomenon has similarly been observed among people searching for health-related information and support such as diabetes awareness, cancer prevention and depression support who were later targeted with advertisements for pharmaceuticals related to these health issues.[28] The propensity for online marketing algorithms to target people at vulnerable moments is particularly harmful.

Proposal 20.9 Require entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals.

We support this proposal. This information should also be publicly accessible to researchers, civil society and government so that profiling and targeting activities are transparent across the system – this will enable better identification of where harmful targeting practices may occur.

Conclusion

This is a critical moment for ensuring that the protections we set up for protecting people's privacy will be fit-for-purpose in a rapidly evolving digital landscape. The health and wellbeing of Australians must always come before the commercial interests. In this context, the harm caused by online platforms and companies selling harmful and addictive products like alcohol through their digital marketing must be addressed. The Privacy Act must ensure that the extensive processing of people's information to profile, track and target them with harmful marketing is prevented.

The Privacy Act can help support a safe digital environment that enables people's health and wellbeing by taking a privacy by design approach and incorporating measures to reduce privacy harms. Pro-privacy default data processing settings, requirements to ensure that data processing practices minimise the risk of adverse impact and harm and are in the best interest of the child, and the introduction of prohibitions for particularly harmful data processing activities will help create a more inclusive online environment that is safer for the whole community.

We thank the Attorney-General's Department for the opportunity to provide input to this consultation on the government response to the Privacy Act Review Report.

References

1. Lensvelt E, Gilmore W, Liang W, Sherk A, T. C. Estimated alcohol-attributable deaths and hospitalisations in Australia 2004 to 2015. Perth: National Drug Research Institute, Curtin University, 2018.

2. Rehm J, Gmel GE, Gmel G, Hasan OSM, Imtiaz S, Popova S, Probst C, Roerecke M, Room R, Samokhvalov AV, Shield KD, Shuper PA. The relationship between different dimensions of alcohol use and the burden of disease—An update. Addiction. 2017;112(6):968-1001.

3. Australian Institute of Health and Welfare. Australian Burden of Disease Study. Impact and causes of illness and death in Australia 2018. Canberra: AIHW, 2021.

4. Whetton S, Tait RJ, Gilmore W, Dey T, Abdul Halim S, McEntee A, Mukhtar A, Abdul Halim S, Roche A, Allsop S, Chikritzhs T. Examining the social and economic costs of alcohol use in Australia: 2017/18. Perth, WA: National Drug Research Institute, Curtin University, 2021.

5. Jernigan D, Noel J, Landon J, Thornton N, Lobstein T. Alcohol marketing and youth alcohol consumption: A systematic review of longitudinal studies published since 2008. Addiction. 2017;112:7-20.

6. Murray R, Leonardi-Bee J, Barker A, Brown O, Langley T. The effect of alcohol marketing on people with, or at risk of, an alcohol problem: A rapid literature review. University of Nottingham & SPECTRUM, 2022.

7. Carah N, Brodmerkel S. Alcohol marketing in the era of digital media platforms. J Stud Alcohol Drugs. 2021;82(1):18-27.

8. Montgomery K, Chester J, Nixon L, Levy L, Dorfman L. Big Data and the transformation of food and beverage marketing: Undermining efforts to reduce obesity? Critical Public Health. 2019;29(1):110-7.

9. Torrance J, John B, Greville J, O'Hanrahan M, Davies N, Roderique-Davies G. Emergent gambling advertising; A rapid review of marketing content, delivery and structural features. BMC Public Health. 2021;21:718.

10. Weber K. Endeavour Group injects $35 million into digital arm. itnews. 2022 Mar 9. Available from: https://www.itnews.com.au/news/endeavour-group-injects-35-million-into-digital-arm-577079?eid=3&edate=20220309&utm_source=20220309_PM&utm_medium=newsletter&utm_campaign=daily_newsletter.

11. Crozier R. Endeavour Group builds an AI-powered personalisation engine. 2021 May 27. Available from: https://www.itnews.com.au/news/endeavour-group-builds-an-ai-powered-personalisation-engine-565124.

12. Evans S. Dan Murphy's loyalists drive Endeavour Group. Australian Financial Review. 2022 Apr 3. Available from: https://www.afr.com/companies/infrastructure/dan-murphy-s-loyalists-drive-endeavour-group-20220331-p5a9lf.

13. World Health Organization. Monitoring and restricting digital marketing of unhealthy products to children and adolescents. Moscow: Regional Office for Europe, 2018.

14. Hootsuite. The Facebook pixel: What it is and how to use it 2021 [updated 2021 Apr 26; cited 2021 Jun 9]. Available from: https://blog.hootsuite.com/facebook-pixel/.

15. Winter S, Maslowska E, Vos AL. The effects of trait-based personalization in social media advertising. Computers in Human Behavior. 2021;114:106525.

16. House A. Dan Murphy's introduces Netflix approach to marketing. Drinks Trade. 2019 Dec 5. Available from: https://www.drinkstrade.com.au/dan-murphys-introduces-netflix-approach-to-marketing?utm_medium=email&utm_campaign=TOP+NEWS%3A+Balter+reveals+plans+to+protect+its+brand+following+CUB+sale&utm_content=https%3A%2F%2F.

17. Foundation for Alcohol Research and Education. Experiences with online marketing of alcohol, gambling and unhealthy food: A survey. Canberra: FARE; 2023 Feb. Available from: https://fare.org.au/experiences-with-online-marketing-of-alcohol-gambling-and-unhealthy-food-a-survey/.

18. VicHealth. Dark marketing tactics of harmful industries exposed by young citizen scientists: VicHealth; 2022. Available from: https://www.vichealth.vic.gov.au/media-and-resources/citizen-voices-against-harmful-marketing.

19. Richmond B. A day in the life of data. Removing the opacity surrounding the data collection, sharing and use environment in Australia. Consumer Policy Research Centre, 2019.

20. Australian Competition and Consumer Commission. Digital platforms inquiry. Final report Canberra: ACCC; 2019. Available from: https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report.

21. Johnson L. With better targeting, alcohol brands bet big on digital: Annual budgets increase as much as 50 percent. Adweek. 2015 Jun 16. Available from: http://www.adweek.com/news/technology/better-targeting-alcohol-brands-bet-big-digital-165357.

22. Davidson D. Facebook targets 'insecure' young people. The Australian. 2017 May 1. Available from: https://www.theaustralian.com.au/business/media/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6.

23. Consumer Policy Research Centre. Not a fair trade: Consumer views on how businesses use their data. 2023 Mar. Available from: https://cprc.org.au/not-a-fair-trade/.

24. Cook M, Mojica-Perez Y, Callinan S. Distribution of alcohol use in Australia. Bundoora: Centre for Alcohol Policy Research, La Trobe University, 2022.

25. Wilson C. Pubs are buying facial recognition technology to track and record you: Crikey; 2022 Aug 10. Available from: https://www.crikey.com.au/2022/08/10/pubs-facial-recognition-surveillance/.

26. United Nations Committee on the Rights of the Child. General comment No. 25 (2021) on children's rights in relation to the digital environment. United Nations, 2021.

27. Elvin S. Fears alcoholics are being 'bombarded' as they struggle to hide Instagram adverts. Metro News. 2021 Mar 10. Available from: https://metro.co.uk/2021/03/10/alcoholics-claim-they-are-struggling-to-hide-adverts-on-instagram-14208953.

28. Morris S. How Big Pharma finds sick users on Facebook: The Markup; 2021. Available from: https://themarkup.org/citizen-browser/2021/05/06/how-big-pharma-finds-sick-users-on-facebook.

Foundation for Alcohol
Research & Education

PO BOX 19 DEAKIN WEST ACT 2600 :: 02 61228600 :: INFO@FARE.ORG.AU :: WWW.FARE.ORG.AU :: ABN 91 096 854 385