Submission on the Privacy Act Review Discussion Paper

January 2022

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 on the use of people's data and personal information to relentlessly target advertising to people based on their vulnerabilities, emotions and other attributes in order 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]

Australians are exposed to advertisements telling them to drink alcohol in a range of settings. Alcoholic products are marketed across television, sports events, in supermarkets, on public transport, and through digital devices such as smart phones and watches that people carry with them throughout the day. This includes children and adolescents who are also exposed to significant amounts of alcohol advertising in Australia.[5-7] Research consistently shows that exposure to advertising for alcoholic products is associated with initiation of alcohol use, and use of higher amounts of alcohol by young people.[5, 8-10]

Government regulation is needed to protect the community from harmful digital marketing practices. The Privacy Act has an important role to play, particularly in addressing some of the most harmful digital marketing practices that are data-driven and enabled through the processing of extensive amounts of data about people.

Complex privacy policies and disingenuous 'consent' mechanisms enable 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.[11-13] This means that intimate information, such as indicators of individuals experiencing addiction or other related mental health challenges, are being used to disproportionately target marketing to people who are most at risk of harm from these products.

The COVID-19 pandemic has provided an unfortunate example of alcohol companies exploiting Australians when they are doing it tough. While the Australian community have been experiencing heighted levels of isolation, anxiety, and economic uncertainty,[14] alcohol companies have been capitalising on the pandemic by promoting alcoholic products as a way to cope with isolation,[15] and driving alcohol into homes through rapid delivery. Advertising alcohol in this way is extremely harmful, as alcohol use contributes to increased stress, anxiety, and depression in the long-term.[16, 17]

A privacy-by-design approach is needed. Being commercially cyberstalked should not be the default when accessing digital environments. People's wellbeing must be prioritised over commercial profits from unfair and harmful data processing and digital marketing practices.

Summary of recommendations

We welcome the opportunity to provide a submission to the Privacy Act review discussion paper consultation.

While we support many of the recommendations within the discussion paper, we submit that there are critical gaps that to be addressed in ensuring that the prohibited practices identified include predatory marketing of harmful products.

Key recommendations that FARE supports

We particularly note our support for the recommendations to:

- Broaden the scope of information captured under the Privacy Act,
- Implement a fair and reasonable requirement whereby companies must ensure that risks of adverse impact and harm are minimised, and the best interests of the child are ensured,
- Implement pro-privacy default settings,
- Provide people with an unqualified right to object to the collection, use and disclosure of their information for marketing purposes, and
- Implement restricted and prohibited practices.

Additional key recommendations

Our key recommendations, which integrate with multiple areas of the Privacy Act under review, but largely fall under the inclusion of prohibited practices are:

- **No use of personal information without voluntary opt-in consent.** The collection, use and disclosure of personal information for commercial marketing purposes must not occur unless a person has provided active, informed, voluntary and non-incentivised opt-in consent.
- **Sensitive information prohibited in marketing.** Even when consent is provided for the collection and use of a person's information for commercial marketing purposes, the collection, use or disclosure of sensitive information for commercial marketing purposes should be prohibited.
- **Predatory profiling of children prohibited.** The tracking, profiling, monitoring or targeting of children for commercial purposes should be prohibited (as per recommendations by the United Nations Committee on the Rights of the Child).[18]
- **Use of children's information for marketing prohibited.** The collection, use or disclosure of children's personal information for commercial marketing purposes should 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.

Submission

Our submission is focused on the role that privacy law plays in protecting people from harmful marketing practices, particularly online. For this reason, our submission does not address all proposals and questions raised in the review discussion paper.

Objects of the Act

Proposal 1.1: Amending the Objects of the Act in Section 2A to clarify the Act's scope and introduce the concept of public interest.

We support this proposal.

It is vitally important to amend the objects in the Privacy Act ('the Act') to make it clearer that the interests of companies should not be balanced against those of individuals when a company is not acting in the public's interest. Protecting people's privacy should be held above protecting the commercial interests of companies, particularly for functions that are not in the public interest, such as the marketing of alcoholic products.

Personal information, de-identification and sensitive information

Proposals 2.1-2.5: Amendments to the definition of personal information and requirement for information to be anonymous before the Act no longer applies.

We support these proposals which will broaden the scope of the information about people regulated under the Act, including technical and inferred personal information which are commonly collected and used for digital marketing practices.

Companies marketing alcoholic products are able target digital marketing to people based on a wide range of information that provide intimate insights into people's lives. The information collected and used for digital marketing activities is widespread and extends beyond the data that people actively provide when using digital platforms. Information that is collected (or inferred) for marketing purposes can include:[12, 19, 20]

- Direct personal identification (e.g., name and date of birth)
- Contact information (e.g., phone number and email address)
- Technical information (e.g., device ID and IP address)
- Location information (e.g., GPS, IP address, mobile sensor data, Wi-Fi access points and Bluetooth)
- Online behaviour (e.g., search history, website visits and products viewed and added to cart)
- Visits to bricks-and-mortar stores (e.g., frequency, length of time spent in store, aisles visited)
- Transactions (e.g., credit card and loyalty/reward card transactions)
- Conversations in the home (e.g., logged through home assistant)
- Biometric information (e.g., stress levels and sleep patterns)
- Other potentially sensitive data (e.g., health information)

Once collected, companies often have broad discretions regarding how a person's information is used and how it is disclosed to third parties.[20] Marketers are able to access sophisticated data analytic systems which combine the large amounts of information collected to track, profile and target people across all devices they use.[12] This enables alcohol marketers to target people with advertising for alcoholic products wherever they go.

Proposal 2.1: Change the word 'about' in the definition of personal information to 'relates to'.

We support this proposal as it more accurately reflects the current nature of data processing for digital marketing purposes.

Proposal 2.2: Include a non-exhaustive list of the types of information capable of being covered by the definition of personal information.

We support this proposal and support the list included in the discussion paper being adopted in the legislation. We particularly support the intention that 'the definition 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 2.3 Define 'reasonably identifiable' to cover circumstances in which an individual could be identified, directly or indirectly. Include a list of factors to support this assessment.

We support this proposal. However, it is unclear how this concept and the proposed list of factors will apply to situations where an individual is distinguished as an individual, or as one of a group of individuals, but where their real-life identity cannot be identified. 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 2.4 Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.

We 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 we know inferred information can be 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.

Consultation question: What do APP entities estimate are the costs and benefits of amending the definition of personal information in the manner suggested?

The proposed amendments to the definition of personal information are important for protecting people's privacy. Any assessment of cost and benefits must assess the cost and benefits to individuals, not just companies, and the cost and benefits in relation to the wider public interest. These costs must be placed above the costs and benefits for commercial entities.

This is especially important when regarding the collection, use and disclosure of personal information for marketing and other commercial purposes. Taken with other recommendations in the review, these changes might impact the targeted marketing capabilities of some companies. However, considering this alone disregards the significant impact that targeted marketing has on people's health and wellbeing, particularly when the products being marketed are addictive and harmful such as alcohol.

Proposal 2.5 Require personal information to be anonymous before it is no longer protected by the Act.

We support this proposal. However, as discussed for proposal 2.3, it is unclear what this means for personal information that may distinguish an individual as an individual, or group of individuals, but where their real-life identity cannot be identified. This is particularly relevant in the digital environment and for digital marketing purposes.

Definition of sensitive information

We support the expanded definition of sensitive information provided in the discussion paper and that these forms of information should be subject to additional protections under the Act. This includes the collection, use and disclosure of location information (which provides extremely intimate and detailed insights in to people's lives as it provides a strong indication of people's preferences and behaviours and enables extremely targeted marketing[12]), financial information (including transactional and thus behavioural information), genomic and biometric information, and health information. We note that the definition of health information must include all information relating to a person's physical, mental, or emotional health and wellbeing.

The processing of sensitive information is of particular concern in relation to commercial marketing, particularly marketing of harmful and addictive products such as alcohol. For example, Instagram has targeted individuals experiencing eating disorders with weight-loss advertisements and weight-loss related search terms such as 'appetite suppressants'.[21] Similarly, people searching health awareness topics such as diabetes awareness, cancer prevention and depression support are documented to have been later targeted with pharmaceuticals for these health issues.[22] In the same nature, we can expect those seeking information for reducing alcohol use or seeking help for alcohol dependence, may also be at heighted risk of receiving alcohol marketing at a time when they are particularly vulnerable to the marketing materials.

Flexibility of the APPs

Proposal 3.1 Amend the Act to allow the Information Commissioner to make an APP code on the direction or approval of the Attorney-General.

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 the proposed additional requirement that this only occur 'where there is unlikely to be an appropriate industry representative to develop the code' be removed. It is critical that alcohol companies are not in charge of creating their own rules for how they process people's personal information.

Privacy regulation should be free from vested corporate conflicts of interest. Currently the requirement under the Privacy Act regarding the development of codes under the Act do not consider the issue of vested corporate conflicts of interest. This is firstly due to the Act requiring the code be developed by industry unless industry refuse to do so, and secondly, conflict of interest is not a consideration required when identifying an appropriate code developer.

Online platforms and companies selling and marketing harmful and addictive products like alcohol have significant vested commercial conflicts of interest when it comes to regulating data processing activities which underpin their current digital marketing models. The current draft Online Privacy Bill, which would see online platforms develop the Online Privacy Code, provides an example of where requiring industry to produce a code under the Privacy Act poses significant risk of undermining the intent of privacy regulation due to vested commercial conflict of interest.

Online platforms have demonstrated that without legal and regulatory measures that set standards for protecting people from extensive data processing and related harms, and that ensure transparency and accountability, they will continue to promote harm through their platforms. They do this by facilitating the targeting by harmful industries of people experiencing vulnerabilities, including children. The vested commercial interests of online platforms conflict with promoting a safe online environment.

This has most recently been made evident by leaked Facebook research and documents that show Facebook is aware of how its platforms harm its users, including children, but refuse to take meaningful actions that counter this because it conflicts with their core business objectives.[23, 24] Speaking to these issues, former employee of Facebook, Frances Haugen, has stated:

> *"The thing I saw at Facebook over and over again, was there were conflicts of interest between what was good for the public and what was good for Facebook. And Facebook, over and over again, chose to optimise for its own interests, like making more money."*[23]

It is evident from past and present examples, that measures developed by industry are ineffective at meeting the needs of the public interest ahead of their corporate interests. In July 2021, ahead of the UK's Age Appropriate Design Code coming into force, Facebook announced that they would "*only allow advertisers to target ads to people under 18 (or older in certain countries) based on their age, gender and location*."[25] Following these claimed changes by Facebook, an investigation by Reset Australia found that Facebook continues to harvest children's data, such as their browsing histories and other online activities, through their Facebook Pixel.[26] The Facebook Pixel provides even more information about individuals than the use of traditional third-party cookie tracking.[27] There is no legitimate reason for Facebook to do this, other than to fuel their advertising delivery system. In effect, the measure taken by Facebook does nothing to prevent their AI systems from identifying, selecting and targeting children that are most likely to interact with an advertisement based on information about their daily activities.

The Australian alcohol industry are also known to seek to prevent, undermine, or delay the introduction of evidence-based regulatory measures,[28, 29] including for marketing regulations.[30, 31] When it is not possible to prevent reforms from occurring, the alcohol industry lobby for and adopt measures that are often ineffective. For example, research has consistently shown that industry codes of practice, such as the Alcohol Beverages Advertising Code Scheme, are ineffective at reducing exposure to alcohol advertising by people most at risk of harm from alcohol use, including young people.[7, 32-34]

The failure of industry codes to effectively prevent harm in the online space has recently been acknowledged in the consultation on the Basic Online Safety Expectations, which raised the need for government development regulations to ensure safe online environments. Similarly, the need to prevent vested commercial conflicts of interest in policy making has recently been acknowledged in the National Preventative Health Strategy 2021-2030, which states that public health policies must be protected from influence by vested and commercial interests (p40).[35]

Notice of collection of personal information

Proposals 8.1-8.4: Introducing clear, specific, standardised notice requirements and strengthening requirements for notices before collection of personal information.

We support these proposals.

Notices and privacy policies are an important source of information for people about 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. The Privacy Act should not solely rely on notices of collection, but these should rather support the broader reforms suggested throughout the review discussion paper.

Proposal 8.1: Introduce an express requirement in APP 5 that privacy notices must be clear, current and understandable.

We support this proposal.

Proposal 8.2: Limiting APP 5 notices to certain matters.

We support this proposal.

Proposal 8.3: Standardised privacy notices could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording and icons.

We support the proposal for standardised privacy notices. While standardised notices are particularly relevant in the online setting, they should not be limited to the organisations covered in the Online Privacy Code. Additionally, given that the Online Privacy Bill is currently drafted to require the code be developed by the industry it aims to regulate, it is important that standardised notices are not developed and designed by industry representatives as their vested commercial interests are too conflicted on this matter. We strongly recommend that 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 comprehension testing.

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.

Proposal 8.4 Strengthen the requirement for when an APP 5 collection notice is required – that is, require notification at or before the time of collection, or if that is not practicable, as soon as possible after collection, unless:

- The individual has already been made aware of the APP 5 matters; or
- Notification would be impossible or would involve disproportionate effort.

We support the intention to strengthen notice requirements to increase transparency, particularly around indirect collection of information.

Consent to collection, use and disclosure of personal information

FARE strongly recommends that the Privacy Act must require that personal information cannot be collected, used or disclosed for commercial marketing purposes unless a person has provided active and expressed consent through an opt-in process that is informed and non-incentivised. This is particularly important in the case of marketing of harmful and addictive products like alcohol.

Where consent is provided, the collection, use and disclosure of personal information must still be subject to additional safeguards in the Act, including a requirement that it be fair and reasonable (particularly that there are no risks of adverse impact or harm and that it is in the best interest of the child), and that prohibited practices are not undertaken. In the case of children, we recommend that the collection, use and disclosure of children's personal information for commercial marketing purposes be a prohibited practice that is not fair and reasonable.

Proposal 9.1 Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.

We support this proposal. 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 Privacy 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, consent is not incentivised or encouraged and provision of the good or service is not conditional on the provision of consent. These protections must ensure that individuals are not required to provide consent for the collection, use and disclosure of their personal information for marketing purposes in order to be provided with a good or service online, and this must be clear when consent is sought, both in terms of the wording of the consent and in the way it is displayed.
- We strongly support the requirement that consent be an unambiguous indication through clear action. This must require individuals to actively express a choice through an opt-in mechanism that clearly separates all consent requirements so that individuals must make an express opt-in choice for each purpose. Bundled consents as part of terms and conditions or as part of a broad category of privacy related consents, or consents displayed in a way that encourages an individual to select the consent option must not be permitted.
- We support the requirement that consent be specific as to what the consent relates to. Where an entity seeks an individual's consent to collect, use or disclose their personal information for the purposes of marketing, specific, unbundled consent must be obtained for that purpose.
- We support a requirement for entities to refresh or renew an individual's consent, if they have opted in to the collection, use or disclosure of their personal information, particularly for sensitive information, or if the collection, use or disclosure practices are for marketing purposes. This is particularly relevant for online platforms.
- Requiring pro-privacy defaults ensures that people can be confident that when they engage with an entity, their data settings will be addressed in a way that best protects their personal information.

Proposal 9.2: Standardised consents could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording, icons or consent taxonomies.

We support the proposal for standardised consents. While standardised consents are particularly relevant in the online setting, they should not be limited to the organisations covered in the Online Privacy Code. Additionally, given that the Online Privacy Bill is currently drafted to require the code be developed by the industry it aims to regulate, we do not support that standardised consents be developed and designed by industry representatives. We recommend that standardised consents are developed by the Information Commissioner in consultation with consumer and data rights groups, designed to facilitate voluntary informed consent and be subject to consumer comprehension testing.

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.

The role of consent

Providing people with real choice and control over the processing of their information is important. However, consent should not be relied on to shift the burden of monitoring and assessing entities data handling practices to individuals. Consent should not be relied on to shift the burden of monitoring and assessing entities data handling practices to individuals.

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 reform suggested throughout the review discussion paper. Particularly, consents should not be able to override other protections or enable harmful data handling processes. The Act's new proposed fair and reasonable requirement and prohibited practices must apply even when consent has been given.

Additional protections for collection, use and disclosure

Proposal 10.1: A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.

We support this proposal.

As the discussion paper notes, 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 appropriate 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 10.2 Legislated factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances could include:

- Whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances,
- The sensitivity and amount of personal information being collected, used or disclosed,
- Whether an individual is at foreseeable risk of unjustified adverse impacts or harm as a result of the collection, use or disclosure of their personal information,
- Whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity,
- Whether the individual's loss of privacy is proportionate to the benefits,
- The transparency of the collection, use or disclosure of the personal information, and
- 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 support the inclusion of the proposed legislated factors relevant to consider in determining whether data processing activities are fair and reasonable and provide further comments on each below. 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 'risk of adverse impact of harm' and 'the best interests of the child' must be minimal requirements.

Foreseeable risk of unjustified adverse impacts 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 and 'do no harm' should be a guiding principle here. We support the intent that this will bring the concept of privacy harms within the Privacy Act and require consideration of potential adverse consequences to either an individual, or society, arising from the processing of personal information. We

agree with the examples that have been provided in the review. We recommend that 'physical or psychological harm' should be broadened to include harm to health and wellbeing in its broad definition.

Best interests of the child: 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. 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 pass the fair and reasonable test (or listed as prohibited practices):

- The profiling or targeting of children for commercial purpose (as per recommendations by the United Nations Committee on the Rights of the Child),[18] 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.

Transparency: Transparency is essential for creating accountability by companies about their data processing activities. More needs to be done to ensure transparent data processing, and we have made suggestions of what this may include in other sections of this submission. However, regarding the fair and reasonable test, while there should be transparency in data processing activities, this transparency should not override harmful data processing activities.

Sensitivity and amount of personal information: We strongly support the intention for this factor to introduce a data minimisation approach, and to ensure that sensitive information, or information relating to an individual's vulnerabilities, should be treated with a higher degree of care. Under the sensitivity factor, processing of sensitive information or information relating to an individual's vulnerabilities should not be considered fair and reasonable.

Proportionality: 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.

Reasonably necessary to achieve the functions and activities: Greater clarity is needed about what this factor would entail. While it is suggested that this would be an objective test, the description provided suggests that this expectation will be inherently subjective. This may result in companies making biased assessments of what a 'reasonable person' might expect. Additionally, 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 sale of personal information. When considering commercial marketing functions and activities, whether the collection, use or disclosure is 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.

Reasonable expectations: 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. Additionally, greater clarity around what the reasonable expectations factor would entail is needed. While it is suggested that this would be an objective test, the description provided suggests that this expectation will be inherently subjective. This may result in companies making biased assessments of what a 'reasonable person' might expect, and might take the assumption that a person has comprehensively read and correctly interpreted privacy policies. Therefore, this factor should not be placed above, or used to balance other factors in the fair and reasonable test.

Consultation Questions: What impacts would the fair and reasonable test have on the business operations of entities?

The fair and reasonable test, particularly the factors relating to ensuring no adverse impact or harm and the best interest of the child, are essential to incorporating privacy harms into the Privacy Act. These factors must be considered even if this poses challenges for companies. 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.

Restricted and prohibited practices

Proposal 11.1: Options 1 and 2 restricted high risk data practices

We support the idea that some data handling practices require additional regulation or should be prohibited entirely. We support the examples provided in the discussion paper of practices that should be considered high risk, though note some of these practices may overlap with those that should be prohibited altogether, not only restricted (see discussion below).

The discussion paper proposes two alternative proposals for the regulation of restricted data practices: additional protections or additional consent requirements. We recommend both be adopted. Responsibility for privacy should not fall solely on individuals. Companies should be responsible for ensuring privacy by design and individuals should also have the capacity to manage privacy related matters.

Where a practice is identified as high risk, both additional protections and additional opt-in consent requirements should be introduced. The additional protections, however, must be the primary means to protect individuals by restricting or regulating high risk practices. The additional consents should provide a further layer of protection on top of these additional protections. In addition to this, people must be provided with an absolute right to not provide consent to their personal information being collected, used or disclosed for restricted purposes.

Prohibited practices

We strongly support the introduction of prohibited practices into the Privacy Act and agree that all practices listed in the discussion paper should be prohibited. In addition, we recommend that the following are included as prohibited practices under the Privacy Act:

- The tracking, profiling, monitoring or targeting of children for commercial purposes (as per recommendations by the United Nations Committee on the Rights of the Child).[18]
- The collection, use or disclosure of children's personal information for commercial marketing purposes, particularly by, or for, companies selling or marketing addictive or harmful products, including alcohol, gambling, tobacco (including e-cigarettes/vapes), and unhealthy food.
- The collection, use of disclosure of sensitive information, such as information related to a person's physical or mental health and wellbeing, for marketing purposes, particularly the marketing of addictive or harmful products.

In our view, these practices are harmful and should be prohibited by being legislated in the Privacy Act. This must be drafted so that entities cannot engage in these practices even if a person where to provide consent. This acknowledges the limited impact of consent requirements, and the necessity of creating a safe online environment that requires people's information to be handled in a way that does not create harm.

Pro-privacy default settings

Proposal 12.1: Introduce pro-privacy defaults on a sectoral or other specified basis.

- Option 1 – Pro-privacy settings enabled by default. Where an entity offers a product or service that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. This could apply to personal information handling that is not strictly necessary for the provision of the service, or specific practices identified through further consultation.
- Option 2 – Require easily accessible privacy settings. Entities must provide individuals with an obvious and clear way to set all privacy controls to the most restrictive, such as through a single click mechanism.

We strongly support option 1. Privacy settings must be pro-privacy and set to the most restrictive for the collection, use and disclosure of personal information that is not strictly necessary for the provision of the service. This should strictly include the collection, use and disclosure of any personal information for commercial marketing purposes. In particular, any consent for the collection, use or disclosure of personal information for the purposes of commercial marketing must have a default setting that consent is not provided, and this can only be changed through an active, informed, freely given and non-incentivised opt-in consent process.

This is a critical element of proposed reforms, as if there is not a requirement for default pro-privacy settings, then the impact of strengthened consent requirements will be limited. To ensure individuals are protected, pro-privacy default settings and opt-in consent must be required in the Act.

Children and vulnerable individuals

Privacy measures regarding children

Proposal 13.1 Amend the Act to require consent to be provided by a parent or guardian where a child is under the age of 16.

Children's personal information should not be collected, used or disclosed for commercial marketing purposes, regardless of parental consent. This is particularly important in the case of marketing for addictive and harmful products including alcohol, gambling, tobacco (including e-cigarettes/vapes), and unhealthy food.

We note that consent, including parental consent, should not be relied on as the primary mechanism to restrict or regulate the actions of entities in handling personal information, particularly in the case of children. The Privacy Act must shift the burden from requiring individuals and parents to examine and evaluate the increasingly complex privacy policies and practices of entities, to requiring entities to collect, use and disclose personal information in a way that will not cause harm and is in the best interests of the child, as discussed further below.

Restricting the collection, use and disclosure of children's personal information

The current ability for the collection, use and disclosure of children's personal information is resulting in the commercial cyberstalking and exploitation of children. 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.

Leaked Facebook documents showed that Facebook gathered psychological insights on almost 2 million children in Australia and New Zealand to sell targeted advertising.[36] This included monitoring children in real time to identify their current mood, including when they feel 'overwhelmed' and 'anxious' to sell targeted advertising.[36] Research has also found Facebook tags children and young people as being interested in harmful products such as alcohol, gambling and junk food,[37, 38] and approves sponsored content promoting

these harmful products to be targeted at children.[38] Further facilitating this harmful marketing to children, Facebook charges approximately $3 for alcohol advertising to be sent to 1000 Australian children aged 13-17 years old.[38]

This results in children being exposed to marketing for harmful products, such as alcoholic products, when they are online.[39] Children's exposure to alcoholic product marketing increases the likelihood that they will start drinking earlier and drink at risky levels.[5] Digital marketing has also been shown to increase positive attitudes and intended and current use of harmful products such as alcohol, tobacco and unhealthy foods.[40]

The proposals in the review discussion paper will ensure companies take more of a privacy by design approach and incorporate measures to reduce privacy harms, which will provide overarching protections that also act to protect children. The introduction of pro-privacy default settings, more appropriately defined and designed consent mechanism, and the reducing risk of adverse impact of harm and the best interests of the child factors in the fair and reasonable test are particularly important in achieving this. We recommend that these should be included in the Privacy Act applying to all entities, not only to organisations addressed in the Online Privacy Code.

When considering what is in the best interest of the child, the Privacy Act should be explicit that regardless of consent, the following are not considered to be in the best interest of the child and should be prohibited:

- The tracking, profiling, monitoring or targeting of children for commercial purposes (as per recommendations by the United Nations Committee on the Rights of the Child).[18]
- The collection, use or disclosure of children's personal information for commercial marketing purposes, particularly by, or for, companies selling or marketing addictive or harmful products, including alcohol, gambling, tobacco (including e-cigarettes/vapes), and unhealthy food.

These overlap with those we have recommended be listed as prohibited practices in the Privacy Act – of course prohibited practices should also not be considered fair and reasonable.

Age verification and parental consent verification

We strongly support the introduction of additional protections applied to children, as discussed above. Children must be defined as people under 18 years of age.

The Online Privacy Bill also proposes to introduce requirements for social media organisations to verify the age of their users, so that children can be provided with additional protections under the Online Privacy Code. The Online Privacy Bill also proposes to verify parental consent for the collection, use and disclosure of children's personal information under the Online Privacy Code.

As we have outlined in the sections above, and in our submission to the Online Privacy Bill, we support an approach that applies protections for children broadly in the Privacy Act, with the Online Privacy Code then supplementing these and providing more detail as applicable in the digital environment. For this reason, the Privacy Act reforms will need to consider how an organisation can and should identify who is a child and is therefore subject to additional protections, and whether this verification is appropriate for all entities or only for online platforms and social media companies.

As we outlined in our submission on the Online Privacy Bill, we support online age verification for social media companies in principle, however any requirement to verify the age of individuals to implement child-specific measures must be subject to strong privacy controls and be distinct from identity verification. Measures taken to verify age 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. To ensure that a privacy preserving system is implemented for age verification, we recommend that

the development of an age verification process be led by the Information Commissioner in consultation with children's and digital rights stakeholders. It must not be led by industry stakeholders who have commercial conflicts of interest on the matter.

Privacy measures regarding 'vulnerable individuals'

The definition and intent of measures around 'vulnerable individuals' has not been well defined in the review discussion paper beyond "individuals with vulnerabilities, including adults experiencing temporary or permanent incapacity for reasons such as disability, illness and injury." In some privacy circumstances, this definition may be appropriate. However, within the context of digital marketing practices, this definition is limited. It does little to address the overarching issue that online platforms are designed in a way that seek to identify and target vulnerabilities through the extensive data collection enables online platforms to develop detailed psychometric profiles on people which are combined with detailed accounts of peoples online browsing behaviour.[41] These insights are used to tailor marketing activities, including marketing content and messaging, towards specific persuasive susceptibilities of individuals.[41]

In the case of alcohol marketing, this ability to prey on people's susceptibilities is particularly harmful as it can disproportionately target people who have are dependent on alcohol. To address the harms of data processing by online platforms, law and regulation must therefore go beyond simply characterising 'vulnerable individuals' and address how the system inherently targets and creates vulnerabilities. Additionally, any measures implemented to protect 'vulnerable individuals' must be done in a way that does not enable or encourage the collection, use or disclosure of additional personal and sensitive information in order to identify a user as vulnerable as this may exacerbate privacy risks.

As discussed in the above section on children, the proposals in the review discussion paper that will ensure companies take more of a privacy by design approach and incorporate measures to reduce privacy harms, will provide overarching protections that also act to protect 'vulnerable individuals.' Particularly, the introduction of pro-privacy default settings, expansion on the definition of sensitive information, and the inclusion of the reducing risk of adverse impact of harm in the fair and reasonable test. To further reduce the risk of companies exploiting or creating vulnerabilities through their data processing practices, we have recommended the following be adopted as a prohibited practice under the Privacy Act: The collection, use of disclosure of sensitive information, such as information related to a person's physical or mental health and wellbeing, for marketing purposes, particularly the marketing of addictive or harmful products.

Right to object and portability and to erasure of personal information

Proposal 14.1 An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information. On receiving notice of an objection, an entity must take reasonable steps to stop collecting, using or disclosing the individual's personal information and must inform the individual of the consequences of the objection.

We support this proposal; however, it must be strengthened. The proposed approach that organisations will be required to 'take reasonable steps' is not sufficient. The Privacy Act must specifically provide that everyone has the right to require organisations not to collect, use or disclose their personal information for the purposes of commercial marketing, and companies must not be able to refuse such a request. This must apply in addition to the consent and notice provisions.

Similar to discussions about consents not being bundled, objections and withdrawals of consent should also not be bundled (either implied or otherwise). For example, if a person wishes to continue to have their location data collected for the purpose of a service functioning but do not wish for their location data to be collected, used or disclosed for other purposes, this should be enabled and clear.

This unqualified right to object should also extend to the collection and use of personal information where it is aggregated with personal information of other users for marketing targeted at groups rather than individuals. This information will still be considered personal information and must also be captured by the right to object.

Proposal 15.1 An individual may only request erasure of personal information where one of the following grounds applies, and subject to exceptions at 15.2, below:

- The personal information must be destroyed or de-identified under APP 11.2,
- The personal information is sensitive information,
- An individual has successfully objected to personal information handling through the right to object (see Chapter 14),
- The personal information has been collected, used or disclosed unlawfully,
- The entity is required by or under an Australian law, or a court/tribunal order, to destroy the information, and
- The personal information relates to a child and erasure is requested by a child, parent or authorised guardian.

We recommend the Privacy Act provide people with a right to request the erasure of any personal information collected, used or disclosed for marketing purposes.

Direct marketing, targeted advertising and profiling

Commercial cyberstalking through online platforms – involving the extensive tracking, profiling and targeting of people for commercial marketing purposes – is a major privacy concern, especially when it comes to children and other people who are vulnerable.

Through extensive data processing, programmatic advertising systems aim to identify people online who are most likely to make a purchase, and to spend higher amounts when doing so.[12, 42, 43] Companies selling and marketing alcohol pay to access these sophisticated digital systems and tools to aggressively market their products that hurt people's health and wellbeing.[11] This means that people who already buy and drink alcoholic products in high amounts are the ones that are targeted most aggressively by alcohol companies through their digital marketing practices.[44]

We strongly recommend that the collection, use or disclosure of personal information for commercial marketing purposes is prohibited unless a person has provided 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. This 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 use a service (as we have discussed in previous sections of this submission).

Additionally, extra protections should be required so that even where consent has been provided for the collection, use and disclosure of personal information for commercial marketing purposes, companies are required to:

- Ensure that their data processing activities meet the fair and reasonable requirement, particularly that they do not pose potential risks of adverse impacts or harm,

- Enable the person to object or withdraw consent at any time and to have information that has been collected for commercial marketing purposes erased, and
- Not process sensitive information, such as factors relating to physical or mental health and wellbeing, whether actual, inferred or generated.

For children, the Privacy Act should explicitly prohibit (regardless of consent):

- The tracking, profiling, monitoring or targeting of children for commercial purposes (as per recommendations by the United Nations Committee on the Rights of the Child),[18] and
- The collection, use or disclosure of children's personal information for commercial marketing purposes, particularly by, or for, companies selling or marketing addictive or harmful products, including alcohol, gambling, tobacco (including e-cigarettes/vapes), and unhealthy food.

Proposal 16.1: unqualified right to object to collection, use or disclosure of personal information for the purposes of direct marketing.

We support this proposal to introduce an unqualified right to object to collection, use and disclosure of personal information for direct marketing. This must be extended to any commercial marketing purposes. We also support a requirement that organisations must advise individuals of this right. This right must apply in addition to the requirement to seek express consent before collecting, using or disclosing an adult individual's personal information for the purposes of commercial marketing.

People should be enabled to easily object to the collection, use and disclosure of their personal information for marketing purposes and to unsubscribe from receiving marketing material, including targeted marketing. Part of enabling people to be able to object to the processing of their information for marketing purposes, is ensuring that marketing is clearly identified as such to people, along with clear and easy mechanisms to object. We recommend this is supplemented with the ability for people to be able to access readily identifiable information about why they are receiving that marketing, including the use of any information about that individual 'whether actual or inferred) that has been used to target marketing to them.

We support the requirement that, on receiving such an objection, the organisation must stop collecting, using or disclosing the individual's personal information for the purpose of commercial marketing. When informing the individual of the consequences of the objection, the consequences must not include that the organisation will cease to provide the individual with the same good or service, unless the provision of direct marketing is the primary good or service provided, and this is clearly identified to the individual. Additionally, the notification of consequences should not mislead people to believe that consent to data processing for marketing purposes is required for a service to function properly/optimally. As provided as an example in the previous section, if a person wishes to continue to have their location data collected for the purpose of a service functioning but do not wish for their location data to be collected, used or disclosed for marketing purposes, this should be enabled. When objecting to or withdrawing consent, it should not be suggested either expressly or implied, that this action will impact the primary functions of the service for which the person has subscribed.

While we support this right to object, this should not replace a model that is designed to protect privacy, where the default position is that consent for the collection, use and disclosure of personal information for marketing purposes is not provided, and is only actively obtained on an informed, voluntary and non-incentivised opt-in basis.

We support this right extending to the collection and use of personal information where it is aggregated with the personal information of other users for marketing targeted at groups rather than individuals. This right

to object must extend to all forms of personal information collected, used or disclosed for the purposes of commercial marketing.

Proposal 16.2: Use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions must be a primary purpose notified to the individual when their personal information is collected.

We agree that the Privacy Act must require organisations to clearly notify individuals that they intend to collect, use or disclose their personal information for the purposes of influencing their decisions or behaviour, and that consent for this must be clearly and separately obtained on a voluntary, informed, non-incentivised opt-in basis. For children, these practices must be prohibited entirely.

It is important that, even where an entity has identified this as a primary purpose and an individual provides consent, the collection, use and disclosure of personal information for this purpose is still subject to additional protections in the Privacy Act, including the fair and reasonable test and prohibited practices. Identifying this as a primary purpose must not be used to support a decision that the practice is appropriate or otherwise compliant with the Privacy Act.

Proposal 16.3: APP entities would be required to include the following additional information in their privacy policy:

- Whether the entity is likely to use personal information, alone or in combination with any other information, for the purpose of influencing an individual's behaviour or decisions and if so, the types of information that will be used, generated or inferred to influence the individual, and
- Whether the entity uses third parties in the provision of online marketing materials and if so, the details of those parties and information regarding the appropriate method of opting-out of those materials.

We support this proposal. However, we note that information in privacy policies should not displace requirements to notify individuals where they intend to collect, use or disclose personal information for commercial marketing purposes, and requirements that active consent is required before data processing activities occur.

Transparency is essential for creating accountability by entities about their data processing activities. In relation to digital alcohol marketing practices, there is little transparency by any actors within the digital marketing ecosystem about the breadth and nature of data collection, use and disclosure for the purposes of marketing alcoholic products. This means the true extent and types of digital marketing practices remains largely under the radar. Similarly, while digital marketing continues to become increasingly personalised, targeted and ephemeral (i.e., content that is shared for limited short periods of time and then disappears), there is little to no transparency about how data-driven digital marketing models function to deliver highly personalised and targeted advertising to people.

Without transparency about the ways in which data is processed through digital marketing models and how this integrates with digital marketing activities (such as the delivery of targeted alcohol marketing), companies are not being held accountable for the harm perpetuated by their digital marketing. In addition to the information proposed in proposal 16.3, we recommend that APP entities also be required to include in their privacy policy information about:

- A description of where personal information is accessed from,
- How the information will be used,
- The quantity and types of third parties' information is share with, and

- For digital marketing activities, an account of the use of any automated decision system to make predictions, recommendations or decisions about which, and how, marketing content is sent to individuals.

Proposal 16.4 Repeal APP 7 in light of existing protections in the Act and other proposals for reform

It is difficult to know whether APP 7 would be rendered obsolete until there is certainty about which changes will be made to the Privacy Act. While many key matters pertaining to data-driven marketing are covered by proposals in the review discussion paper and further recommendations we have made, the inclusion of a privacy principle dedicated to the topic of marketing helps ensure marketing related privacy issues remain front of mind in privacy considerations. Additionally, if all of the suggested amendments don't make it through to the final changes, then there may be gaps or unintended consequences of repealing APP7. A decision on this issue should only be made once all other amendments to the Act are finalised and it is clear that there will be no gaps in protection caused if it is repealed.

Consultation question: Should express consent be required for any collection, use or disclosure of personal information for the purpose of direct marketing?

Yes. This must be extended to all commercial marketing. The collection, use and disclosure of personal information for commercial marketing purposes must not occur unless a person has actively provided voluntary, informed, non-incentivised opt-in consent.

However, for children the collection, use or disclosure of their personal information for commercial marketing purposes must be prohibited, regardless of the child or parent's consent. Particularly, for by or for companies selling and marketing addictive and harmful products including alcohol, gambling, tobacco (including e-cigarettes/vapes), and unhealthy food.

Consultation question: What are some of the practical challenges of implementing a global opt-out process, to enable individuals to opt out of all online tracking in one click?

We strongly support a pro-privacy approach whereby the default setting is that consent is not assumed for online tracking and data processing for commercial marketing purposes. Consent must be express and provided on a voluntary, informed, non-incentivised opt-in basis, and must be provided for each entity for each specific purpose. We do support a global process where adults can register that they never provide consent for the collection, use and disclosure of their personal information for commercial marketing purposes, but this must not replace pro-privacy defaults and must never apply to enable global opt-in consent.

Consultation question: Should the unqualified right to object to marketing extend to the collection and use of personal information where it is aggregated with the personal information of other users for marketing targeted at cohorts rather than individuals?

We support this right extending to the collection and use of personal information where it is aggregated with the personal information of other users for marketing targeted at groups rather than individuals. This right to object must extend to all forms of personal information collected, used or disclosed for the purposes of commercial marketing.

Consultation question: Do customer loyalty schemes offer more tangible benefits to consumers, and should they be regulated differently to other forms of direct marketing?

We support these being subject to the same regulation as other forms of personal information, with further regulation in addition if required.

Accessing and correcting personal information

Proposal 18.1: An organisation must identify the source of personal information that it has collected indirectly, on request by the individual, unless it is impossible or would involve disproportionate effort.

We support the Privacy Act providing individuals with the right to obtain information about the source from which their personal information was obtained. This must include all forms of personal information, including inferred and generated information. Individuals must be able to access clear information on why they are receiving certain marketing, particularly in a digital environment, and on what information has been collected, used and disclosed in relation to them that has resulted in their exposure to particular marketing.

Regulation and enforcement

We support the proposed reforms to strengthen the enforcement and compliance provisions of the Act, set out in proposals 24.1 and 24.2 and 24.4 that would:

- Create tiers of civil penalty provisions to extend civil penalties to breaches beyond those that are serious or repeated,
- Clarify what is considered a 'serious' or 'repeated' interference with privacy (we support the suggestions for what breaches might be captured here), and
- Provide the Information Commissioner the power to undertake public inquiries and reviews into specific matters.

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. People, and the health and wellbeing of Australian society, must always come before 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 personal information and data 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 review of the Privacy Act.

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. Vanderberg B, O'Brien K. Report on the extent, nature, and consequences of children and young people's exposure to alcohol advertising and sponsorship. Monash University, 2020.

7. Aiken A, Lam T, Gilmore W, Burns L, Chikritzhs T, Lenton S, Lloyd B, Lubman D, Ogeil R, Allsop S. Youth perceptions of alcohol advertising: are current advertising regulations working? Australian and New Zealand journal of public health. 2018;42(3):234-9.

8. Hastings G, Anderson S, Cooke E, Gordon R. Alcohol marketing and young people's drinking: A review of the research. Journal of public health policy. 2005;26(3):296-311.

9. Smith LA, Foxcroft DR. The effect of alcohol advertising, marketing and portrayal on drinking behaviour in young people: systematic review of prospective cohort studies. BMC Public Health. 2009;9(1):51.

10. Meier P, Booth A, Stockwell T, Sutton A, Wilkinson A, Wong R, Brennan A, OÆReilly D, Purshouse R, K. T. Independent review of the effects of alcohol pricing and promotion. Part A: Systematic reviews. Sheffield: University of Sheffield, 2008.

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

12. 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.

13. 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(1).

14. Newby JM, O'Moore K, Tang S, Christensen H, Faasse K. Acute mental health responses during the COVID-19 pandemic in Australia. PLOS ONE. 2020;15(7):e0236562.

15. Foundation for Alcohol Research and Education, Cancer Council Western Australia. An alcohol ad every 35 seconds. A snapshot of how the alcohol industry is using a global pandemic as a marketing opportunity. Canberra: FARE & CCWA, 2020.

16. Borges G, Bagge CL, Cherpitel CJ, Conner KR, Orozco R, Rossow I. A meta-analysis of acute use of alcohol and the risk of suicide attempt. Psychol Med. 2017;47(5):949-57.

17. National Health and Medical Research Council. Austrlaian Guidelines to Reduce Health Risks from Drinking Alcohol. Canberra: Commonwealth of Australia, 2020.

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

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.

21. Hern A. Instagram apologises for promoting weight-loss content to users with eating disorders. The Guardian. 2021 Apr 15. Available from: https://www.theguardian.com/technology/2021/apr/15/instagram-apologises-for-promoting-weight-loss-content-to-users-with-eating-disorders.

22. 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.

23. Paul K, Milmo D. Facebook putting profit before public good, says whistleblower Frances Haugen. The Guardian. 2021 Oct 5. Available from: https://www.theguardian.com/technology/2021/oct/03/former-facebook-employee-frances-haugen-identifies-herself-as-whistleblower.

24. Milmo D, Paul K. Facebook disputes its own research showing harmful effects of Instagram on teen's mental health. The Guardian. 2021 Sep 30. Available from: https://www.theguardian.com/technology/2021/sep/29/facebook-hearing-latest-children-impact.

25. Facebook. Giving young people a safer, more private experience. 2021 Jul 27. Available from: https://about.instagram.com/blog/announcements/giving-young-people-a-safer-more-private-experience.

26. Yi-Ching E, Farthing R. How Facebook still targets surveillance ads to teens. Reset Australia, Fairplay and Global Action Plan, 2021.

27. Semerádová T, Weinlich P. Computer estimation of customer similarity with Facebook lookalikes: Advantages and disadvantages of hyper-targeting. IEEE Access. 2019;7:153365-77.

28. Foundation for Alcohol Research and Education. Alcohol industry fingerprints: Analysis of modifications to the national alcohol strategy. 2019.

29. Bartlett A, McCambridge J. Doing violence to evidence on violence? How the alcohol industry created doubt in order to influence policy. Drug and Alcohol Review. 2021.

30. Stafford J, Chikritzhs T, Pierce H, Pettigrew S. An evaluation of the evidence submitted to Australian alcohol advertising policy consultations. PLOS ONE. 2021;16(12):e0261280.

31. Martino FP, Miller PG, Coomber K, Hancock L, Kypri K. Analysis of Alcohol Industry Submissions against Marketing Regulation. PLOS ONE. 2017;12(1):e0170366.

32. Noel JK, Babor TF, Robaina K. Industry self-regulation of alcohol marketing: a systematic review of content and exposure research. Addiction. 2017;112:28-50.

33. Pierce H, Stafford J, Pettigrew S, Kameron C, Keric D, Pratt IS. Regulation of alcohol marketing in Australia: A critical review of the Alcohol Beverages Advertising Code Scheme's new Placement Rules. Drug and Alcohol Review. 2019;38(1):16-24.

34. Noel JK, Babor TF. Does industry self-regulation protect young people from exposure to alcohol marketing? A review of compliance and complaint studies. Addiction. 2017;112:51-6.

35. Department of Health. National Preventative Health Strategy 2021-2030. Canberra: Australian Government, 2021.

36. 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.

37. Hern A, Ledergaard F. Children 'interested in' gambling and alcohol, according to Facebook. The Guardian UK. 2019 Oct 10. Available from: https://www.theguardian.com/technology/2019/oct/09/children-interested-in-gambling-and-alcohol-facebook.

38. Williams D, McIntosh A, Farthing R. Profiling children for advertising: Facebook's monetisation of young people's personal data. Sydney: Reset Australia, 2021.

39. VicHealth. Under the radar: Harmful industries' digital marketing to Australian children. Melbourne: A report prepared by the Victorian Health Promotion Foundation, 2020.

40. Buchanan L, Kelly B, Yeatman H, Kariippanon K. The effects of digital marketing of unhealthy commodities on young people: A systematic review. Nutrients. 2018;10(2):148.

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

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

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

44. 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.

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