Obesity Policy Coalition: Submission on Privacy Act Review
December 2021

Background

The Obesity Policy Coalition (OPC) is a partnership between Cancer Council Victoria, Diabetes Victoria, VicHealth and the Global Obesity Centre at Deakin University; a World Health Organization (WHO) Collaborating Centre for Obesity Prevention. The OPC advocates for evidence-based policy and regulatory change to address overweight, obesity and unhealthy diets in Australia, particularly among children. We welcome the opportunity to provide feedback on the review of the Privacy Act (the Act).

The OPC's key focus in this area is on the use of children's data and personal information to market harmful products, including unhealthy food and drinks. Children should be able to use digital media without being exposed to marketing that is harmful to their health, including for unhealthy food. We know that digital media is an important part of children's daily lives, with Australian children going online as part of their education, to access information of all kinds, to communicate with their friends and family, and to have fun.

Instead of an environment that promotes their health and wellbeing, when children go online they are often bombarded with sophisticated digital marketing campaigns for unhealthy food. These campaigns use technologies and delivery systems designed and supported by powerful online platforms and social media companies, to harness children's data and personal information to enable marketing to be highly targeted, engaging and effective.

There is clear and robust evidence that children's exposure to unhealthy food marketing influences their food choices, influences their diets, and can contribute to poor diets, overweight and obesity. Despite Australian children's high rates of overweight and obesity, there are few controls on advertising practices targeting advertisements for unhealthy foods and beverages to children in Australia.

Government must step in to put children's health before the profits of global online platforms and processed food companies and enact higher standards to create an online environment that supports health and wellbeing and reduces harm. While we strongly advocate for broad government regulation to ensure children are fully protected from digital marketing for unhealthy food, we support the role of privacy law in contributing to this outcome.

The Privacy Act has an important role to play in protecting children online and creating an environment that restricts commercial exploitation of children and enables children to participate as digital citizens, while having their best interests protected. Our community expects and supports government action in this area.

OPC supports the need for reform

The OPC strongly supports a strengthened Privacy Act to better protect children from harmful data practices, including the collection, use and disclosure of their personal information to market harmful industries such as unhealthy food, alcohol and gambling.

This is primarily an issue relating to digital marketing. There are few protections in place to regulate data practices to prevent children from being exposed to predatory marketing practices online. The digital marketing model collects, uses and discloses large amounts of personal information, including specific information about an individual's online behaviour, purchase preferences, social networks and physical location.[1] This information is being used by marketers, including corporations who market unhealthy food, to target their marketing directly to particular groups of consumers, including children, based on their individual profiles.[2] This collection, use and disclosure of personal information and online activity is a significant risk to children's privacy, health and wellbeing, particularly as it is difficult to monitor and to prevent.

The protection of children's privacy in Australia, particularly online, lags behind international standards[3] and we support reform to better protect Australian children. As well as protecting children, we support wider reform for all Australians, to better protect individual privacy and reduce the risk of harm, particularly in the digital environment.

We support amendments to the Privacy Act and consider that changes to the Act should be the primary mechanism to protect individuals when online, particularly children. This is because reform to the Privacy Act is required to make significant fundamental change to the way personal information is defined and protected in Australia, and to set out certain types of data handling practices that are not permitted by any organisations.

We also support the introduction of the Online Privacy Bill and the development of an Online Privacy Code for large online platforms, data brokerage and social media companies, however the Privacy Act reforms should take precedence, with these instruments then supplementing and strengthening general protections contained in the Privacy Act in the context of the digital environment. For this reason, many recommendations made in this submission reflect our views on the Online Privacy Bill.

Submission

We note that our submission is focused on proposals and issues that are related to OPC's key focus of protecting children from unhealthy food marketing, and the role that privacy law plays in protecting children from harmful marketing and harmful marketing practices, particularly online.

For this reason, our submission does not address all proposals and questions raised.

[1] World Health Organisation Regional Office for Europe, *Tackling food marketing to children in a digital world: trans-disciplinary perspectives* (2016), page 8.
[2] World Health Organisation Regional Office for Europe, *Tackling food marketing to children in a digital world: trans-disciplinary perspectives* (2016), pages 8-9.
[3] For example, the GDPR in Europe and the Children's Online Privacy Protection Act of 1998 in the United States.

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.

In particular, we support clarifying that the protection of individuals' privacy should only be balanced with the interests of entities in carrying out their functions or activities to the extent they are undertaken in the public interest. For example, we do not support balancing protection of privacy against an entity's functions that, while they may serve that entity well in terms of increasing their revenue, are not in the best interests of the individual or the public more generally, such as marketing harmful products.

Definition of personal information

Proposals 2.1-2.3: Amendments to the definition of personal information

We support these proposals, particularly:

- amending the definition of personal information to make it clear that it includes technical and inferred personal information as these represent key forms of personal information collected, used and disclosed in the digital environment, in particular for the purposes of commercial marketing. If these forms of information are not captured in the definition of 'personal information' then this will severely limit the impact of any additional protections put in place in the digital environment, including in relation to children.

- including a non-exhaustive list of the types of information that can fall within the definition, as well as a list of objective factors to assist APP entities to determine when an individual is reasonably identifiable.

- It is important that the concept of 'reasonably identifiable' is sufficiently broad in the Act to capture the ways that information about individuals is used to target marketing to them. It must capture situations where a person is identified as an individual, or as a person belonging to a group of individuals with certain characteristics, even where the real-life identity of the person cannot be established. It is critical that the definition is sufficiently broad to capture this and to capture the current ways that information is used to target marketing to individuals, such as the creation of lookalike audiences, as well as how that may be done in the future. If this is not done, then any additional protections included in the Act, in particular in relation to marketing practices, are unlikely to have any meaningful effect.

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

We support this proposal.

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. In particular, we support the view in the discussion paper 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.

We support this proposal, however it is unclear to us 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.

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 has particular relevance to protections that apply in relation to the collection, use or disclosure of personal information for the purposes of marketing, as we know inferred information can be used by platforms and advertisers to market harmful products to individuals, including children, on the basis of inferred information. This must capture current practices, such as the creation of lookalike audiences.

Proposal 2.6 Re-introduce the Privacy Amendment (Re-identification) Offence Bill 2016 with appropriate amendments

We support this proposal.

Definition of sensitive information

We support an expanded definition of sensitive information, though we note that the impact and necessity of this will depend on other amendments to the Act and their relationship to this definition. Some of the intrusive practices discussed in the context of the definition of sensitive information, such as collection of location information, may be able to be dealt with in a different way, such as including it as a prohibited practice, or a restricted practice subject to strong controls. We note that the collection, use and disclosure of sensitive information is of particular concern in relation to commercial marketing, including marketing to children, and in particular in relation to the marketing of harmful products.

With that in mind, we agree that there are certain things that meet the requirement of being 'sensitive information' and should therefore be subject to additional protections in an appropriate form. These include location information, financial information (including transactional information), genomic and biometric information and a broad concept of health information which must include all information relating to a person's physical, mental or emotional health or wellbeing.

Flexibility of APPs

Proposal 3.1: Improving the OAIC's ability to make codes

We support the proposal to amend the 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 this be the only requirement, and that the proposed additional requirement that it only occur 'where there is unlikely to be an appropriate industry representative to develop the code' is not included.

The Information Commissioner should have a clear power to make or amend an APP Code where it is in the public interest, even where there is an industry representative who would like to develop the APP Code.

We note that, as outlined in our submission on the Online Privacy Bill (OP Bill), we recommended that the OP Bill provide the Information Commissioner with the power to develop the OP Code even if there is an appropriate industry organisation that is willing to do so.

Proposal 3.2: Amend the Act to allow the IC to issue a temporary APP code on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.

We support this proposal.

Small business exemption

We support changes to the current small business exemption to substantially expand the coverage of the Act to smaller businesses.

The OPC's focus is on ensuring that protections that regulate the way that entities collect, use and disclose personal information for commercial marketing purposes, including in relation to children, also apply to small business. The impact of marketing practices on individuals, especially in relation to children and as applied to marketing for harmful products including unhealthy food, alcohol and gambling, are not removed or necessarily reduced in the case of a small business. This is particularly the case for digital marketing, where even small businesses are able to make use of the powerful digital marketing models of major digital platforms to ensure their marketing has maximum reach and impact. The Act must protect Australians from these practices as appropriate, regardless of business size.

Notice of collection of personal information

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 this proposal and recommended that standardised notices be included as part of the Online Privacy Code. Standardised notices must be developed by the Information Commissioner in consultation with consumer and data rights groups, designed to reduce notice fatigue and be subject to consumer comprehension testing. It is important to consider how this notice requirement interacts with consent requirements. These two elements may need to be

combined in many cases, and design of these standardised notices must be undertaken to ensure consumers are not incentivised or otherwise encouraged to consent by the way the notice is designed. Care would also need to be taken that any deviation from the standard notification were adequately highlighted.

Proposal 8.4 Strengthen the requirement for when an APP 5 collection notice is required

We support the intention to strengthen notice requirements to ensure they are more likely to be read and understood. It is not entirely clear to us, however, what the practical implications of this will be.

Consent to the collection, use and disclosure of personal information

Consent for the collection, use and disclosure of an adult's personal information for commercial marketing purposes

OPC strongly advocates that the Act must include a requirement that an adult individual's personal information cannot be collected, used or disclosed for the purposes of commercial marketing without express consent. This is particularly important in the case of commercial marketing for harmful products, including unhealthy food, alcohol and gambling. Even where consent is provided, the collection, use and disclosure of personal information for that purpose must be subject to additional safeguards in the Act, including a requirement that it be fair and reasonable, 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 is a prohibited practice that is not considered 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. We recommend that these terms be subject to further definition and clarification to ensure they are meaningful in practice. 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, other than those required to provide

the good or service. 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-consumer defaults ensures that individuals 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. This provides an additional protection for individuals who may have consent fatigue and may not take the time to adjust their settings.

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 this proposal, and recommended standardised consents be included as part of the Online Privacy Code. Standardised consents must be developed by the Information Commissioner in consultation with consumer and data rights groups, designed to reduce consent fatigue and be subject to consumer comprehension testing. It is important to consider how this consent requirement interacts with notice requirements. These two elements may need to be combined in many cases, and design of these standardised consents must be undertaken to ensure consumers are not incentivised or otherwise encouraged to consent by the way the notice is designed. Care would also need to be taken that any deviation from the standard notification were adequately highlighted.

The role of consent

Overall, we support the proposed measures to strengthen consent requirements in the Act. We do note, however, that consent should not be the primary mechanism to restrict or regulate the actions of entities in handling individuals' personal information. Consent should not be relied on to shift the burden of monitoring and assessing entities data handling practices to individuals.

Consent should be required, and has an important role, but the entire system must be designed not to encourage or incentivise consent, and not to allow consent to override other protections and enable data handling practices that are not in an individual's best interests, not in keeping with community expectations, and not required for an organisation's legitimate interests. The Act's new proposed fair and reasonable requirement and prohibited practices must apply even where consent has been given. The Act must create a system that is designed to preserve privacy and prevent harm and only to allow practices that do not unduly impact privacy or cause harm, even where consent has been provided.

Additional protections for collection, use or disclosure of personal information

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 individuals' personal information is an important step in shifting the burden of examining and evaluating privacy practices away from individuals and giving entities 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 c We support the inclusion of the proposed legislated factors relevant to whether it is fair and reasonable in the circumstances, subject to the following comments:

- We strongly support a requirement for children that collection, use or disclosure of a child's personal information will only be considered fair and reasonable where it is in the child's best interests. We recommend this be an overarching test for the handling of children's personal information, meaning that if collection, use or disclosure of a child's personal information is not in their best interests, it must not be permitted.

  We recommend the concept of a child's 'best interests' then be subject to further definition, with the Act including a non-exhaustive list of practices that will not be in a child's best interests. It must be clear that it will not be in a child's best interests, and therefore not fair and reasonable, to:

  - collect, use or disclose their personal information for the purposes of commercial marketing, particularly marketing for harmful products including unhealthy food, alcohol and gambling. There may be a need for limited exceptions that do not apply to harmful products. See further discussion on this relating to specific protections for children on page 12.
  - collection, use or disclosure of children's personal information by harmful industries, including unhealthy food and drinks, alcohol and gambling, for the purposes of analysing or influencing children's behaviour or decisions in any circumstances.
  - track, profile and monitor children's behaviour for commercial purposes

- We strongly support the inclusion of a factor related to privacy harms, about 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. We agree with the examples of 'risk and adverse impact or harm' that have been listed in the discussion paper but recommend that harm to health and wellbeing be added as a distinct factor.

- We support the inclusion of the sensitivity and amount of personal information being collected, used or disclosed, and agree with the promotion of a data minimisation approach.

- We support the inclusion of a 'reasonable expectations' factor, but note it is important that this is interpreted by reference to the consumer's primary purpose in engaging with

the entity, and not by reference to common intrusive data handling practices, particularly in relation to digital marketing. The ways that data can and is often used for the purposes of digital marketing should not be the determinative factor when assessing an individual's reasonable expectations.

- We support the inclusion of a factor about the collection, use or disclosure being reasonably necessary to achieve the functions and activities of the entity, however this must be strengthened to ensure it only captures the subset of those functions that are legitimate or necessary. However this is framed, it must be clear that commercial marketing or the sale of data to a third party should not be considered a necessary or legitimate function or activity, unless that is the primary purpose of the entity and the reason why the individual has requested the good or service.

- We support the inclusion of a factor around transparency of collection, use or disclosure of personal information, although we note that a high standard of transparency should be a minimum standard and transparency should not result in data handling practices that would otherwise not be fair and reasonable being accepted. This factor should be focused on identifying data handling that is not fair and reasonable.

- We support the inclusion of a factor around proportionality, and in particular a focus on data minimisation and whether the same outcomes can be achieved in a less intrusive way. We are concerned, however, at how this factor may be interpreted in light of the marketing model of online platforms and social media companies in particular, where services are provided without charge with user data being collected, used and disclosed on a large scale to generate income. The perceived benefits of participating in social media and other online platforms do not justify inappropriate data handling practices.

Overall, we support this approach and the majority of these factors, however it is not clear to us how they would all be balanced in practice and what role each factor would play. In our view, some factors should take precedence over others and we recommend an approach that considers this. For example, the best interests of the child and risk of harm should come before others. Some factors must not be used to identify otherwise 'unfair' data handling practices as fair and reasonable, including factors around proportionality, reasonable expectation and transparency. These factors, however, represent a minimum standard for data handling and have an important role to play in identifying practices that are not fair and reasonable.

10.3 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. We support this proposal.

Restricted and prohibited acts and 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. 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, individuals must be provided with an absolute right not to 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 Act and agree that all practices listed in the discussion paper should be prohibited.

In addition, we support the inclusion of the following as prohibited practices:

- collection, use and disclosure of children's personal information for the purposes of commercial marketing, particularly marketing by harmful industries, including unhealthy food and drinks, alcohol and gambling. For marketing that is not for harmful products, some limited exceptions may be appropriate where such practices might overall be in children's best interests and do not put children at risk of harm. For example, public health social marketing campaigns.
- collection, use or disclosure of children's personal information by harmful industries, including unhealthy food and drinks, alcohol and gambling, for the purposes of analysing or influencing children's behaviour or decisions in any circumstances.
- tracking, profiling, or monitoring the behaviour of children for commercial purposes, or similar practices.
- collection, use or disclosure of personal information related to a person's physical or mental health and wellbeing or financial situation, for the purposes of marketing harmful products.

In our view, these practices are harmful and should be prohibited by being legislated in the Act. This must be drafted so that entities cannot engage in these practices even if individuals or parents provide consent. This acknowledges the limited impact of consent requirements, and the necessity of creating a safe online environment that requires data 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 Option 2 – Require easily accessible privacy settings We support option 1. We support requirements to establish default privacy settings that are pro-privacy and set to the most restrictive options to collect, use or disclose an individual's personal information. 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 a clear, voluntary, opt-in consent process (for adults – entities should not be able to collect, use or disclose children's personal information for commercial marketing purposes so consent cannot be sought).

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. This is because consent fatigue is likely to mean that many individuals consent to default settings without detailed consideration. To ensure individuals are protected, pro-privacy default settings and opt-in consent must be required in the Act. Of course, there will often be some collection, use or disclosure of personal information that is minimally required to provide a good or service, and different default settings may be **appropriate** in those cases.

Children and vulnerable individuals

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. Option 1 – All collections of personal information Parent or guardian consent to be required before collecting, using or disclosing personal information of the child under the age of 16. • Option 2 – Where consent is currently required under the Act Parent or guardian consent to be required in respect of a child under the age of 16 in situations where the Act currently requires consent

Our overarching position is that children's personal information should not be collected, used or disclosed for commercial marketing purposes and that this prohibition cannot be overridden by parental consent. This prohibition is particularly important in the case of marketing for harmful products, including unhealthy food, alcohol and gambling.

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 individuals' personal information, particularly in the case of children. The 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 is fair and reasonable and in children's best interests, as discussed further below.

Proposal 13.2 Require APP 5 notices to be clear, current and understandable, in particular for any information addressed specifically to a child.

We support APP 5 notices being clear and understandable for children in general.

Limits on collections, use and disclosure of children's personal information

OPC strongly supports the introduction of strong controls on how children's personal information is collected, used and disclosed. It is important to create strong protections for children that protect the collection, use and disclosure of their personal information where it is not in their best interests, and that apply independently of consent either from the child or their parent/guardian.

We support the introduction of the fair and reasonable test in relation to children, where the primary consideration is whether the collection, use and disclosure of the child's personal information is in their best interests (fair and reasonable/best interests of the child test), and recommend this be included in the Privacy Act applying to all entities and not only to online platforms through the Online Privacy Code. This must be an overarching test/requirement and not only a factor to be taken into account.

We recommend the Act clearly outline some forms of data handling that do not meet this test and will not be considered fair and reasonable in relation to children. These overlap with those we have recommended be listed as prohibited practices in the Act – of course prohibited practices will also not be considered fair and reasonable in relation to children.

We support the list in the discussion paper that includes online tracking, behavioural monitoring and profiling of children, the disclosure of a child's personal information to a third party which exposes the child to potential safety or privacy risks, and the sale of a child's personal information.

In our view, the following practices must also be considered not to meet the fair and reasonable/best interests of the child test:

- collection, use and disclosure of children's personal information for the purposes of commercial marketing, particularly marketing by harmful industries, including unhealthy food and drinks, alcohol and gambling.

  For marketing that is not for harmful products, some limited exceptions may be appropriate where such practices might overall be in children's best interests and do not put children at risk of harm. For example, public health social marketing campaigns.

- collection, use or disclosure of children's personal information by harmful industries, including unhealthy food and drinks, alcohol and gambling, for the purposes of analysing or influencing children's behaviour or decisions in any circumstances.

- tracking, profiling, or monitoring the behaviour of children for commercial purposes, or similar practices.

The Act must clearly list the above practices as not being fair and reasonable in relation to children, with no opportunity for flexible interpretation in those situations.

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 individuals under 18.

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

As we outline in this submission and in our submission on the OP Bill, we support an approach that applies protections for children broadly in the Privacy Act, with the OP Bill and OP 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 OP Bill, we support online age verification for social media companies in principle, however it must be subject to strong privacy controls. Age verification must not be designed in a way that encourages organisations to collect even more

information to verify the age of users. We support proportional measures that effectively verify that an individual is over 18, but do not require individual users to be identified online, and do not require the retention of data used to verify age. Due to the potential issues involved with age verification, this process should be developed by government, in consultation with stakeholders, rather than developed by online platforms.

As online age verification is an issue that has a broad application beyond the OP Code, we recommend the Australian Government develop agreed national standards for online age verification that can apply for this and for other purposes. The detail of how verification can be effectively and practically achieved in different circumstances while preserving privacy and the ability to engage online anonymously can then be developed with stakeholder engagement and consumer testing as appropriate.

We also support the requirement to obtain verified parental consent for children under 18 on social media, although we have similar concerns as in relation to age verification. Any parental consent process must be subject to the same strong privacy controls.

Vulnerable individuals

Protecting vulnerable individuals is important, however this 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.

We recommend protections be introduced that address the marketing model and the way it collects, uses and discloses personal information that may target particular individuals in a way that may be more likely to result in harm. This is particularly the case for marketing of harmful products. For example, we recommend that the Privacy Act be amended to prohibit the collection, use or disclosure of personal information related to a person's physical or mental health and wellbeing or financial situation, for the purposes of marketing harmful products.

Right to object and portability

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 Act must specifically provide that all individuals have the right to require organisations not to collect, use or disclose their personal information for the purposes of commercial marketing, and organisations 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 an individual 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.

Right to erasure of personal information

Proposal 15.1 An individual may only request erasure of personal information where one of the listed grounds applies, and subject to exceptions at 15.2, We recommend the Act provide individuals with a right to request the erasure of any personal information collected, used or disclosed for the purposes of marketing.

Direct Marketing

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

We support proposal 16.1, that the right to object must include an unqualified right to object to any collection, use or disclosure of personal information for the purposes of 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.

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 and must inform 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.

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 obtained (for adults) on a clear, specific, voluntary and 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 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 (for adults) must be clearly and separately obtained on a

voluntary, specific, unincentivised, 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 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 Act.

Proposal 16.3: APP entities would be required to include the listed additional information in their privacy policy We support this proposal, however we consider an entity must be required to notify individuals if it intends to use personal information for the purposes of influencing an individual's behaviour or decisions for commercial purposes. Entities must be required to seek express, specific, voluntary consent to collect, use or disclose an adult individual's personal information for the purposes of commercial marketing.

We recommend that APP entities also be required to include in their privacy policy information about how the information will be used, and that for digital marketing this should extend to information about the use of any automated system to predict, recommend or profile an individual and to decide how marketing content is sent to an individual. Entities should also be required to provide information about how this is used, including an account of the companies' use of any automated decision system to make predictions, recommendations or decisions about which and how marketing content is sent to individuals.

We support the requirement to provide information about the use of third parties in the provision of online marketing materials, but recommend this include the quantity and types of third parties the information is shared with.

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

OPC does not have a final view on this issue at this stage. We note that 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.

General comment on direct marketing

OPC makes the following points in response to the discussion paper questions on direct marketing:

- **Express consent:**
    - For adults: Yes, express consent must be required for any collection, use or disclosure of personal information for the purposes of direct marketing. This must be extended to all commercial marketing and must require clear, voluntary, specific and unincentivised consent provided on an opt-in basis. This must apply only to adults.

    - For children: the collection, use or disclosure of their personal information for the purposes of commercial marketing, in particular for harmful products such as unhealthy food, alcohol and gambling, must be prohibited.

- **Global opt-out process for online tracking:** We support an approach where the default setting is that individuals do not consent to online tracking, and to the collection, use and disclosure of their personal information for commercial marketing purposes. Consent must be express and provided on a voluntary, specific and unincentivised 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 never apply to enable global opt-in consent.
- **Unqualified right to object to marketing:** 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.
- **Customer loyalty schemes:** 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 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 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.

Proposal 18.3: Changes to process to access personal information.

We support this proposal.

Organisational accountability and overseas data flows

OPC supports measures to strengthen organisational accountability, to ensure that the obligations in the Act are implemented and monitored by organisations appropriately. We also support measures to ensure that personal information that is disclosed overseas is subject to the protections in the Privacy Act, particularly in relation to marketing and in relation to children.

Regulation and enforcement

Enforcement and compliance

We support the proposed reforms to strengthen the enforcement and compliance provisions of the Act, set out in proposals 24.1, 24.2, 24.4, 24.5, 24.6.