Submission from the Interactive Advertising Bureau (IAB) Australia

Response to the Attorney-General's Department

Privacy Act Review Discussion Paper

24th January 2022

Contents

About IAB Australia

The Interactive Advertising Bureau (IAB) Australia Limited www.iabaustralia.com.au is the peak trade association for digital advertising in Australia.

IAB Australia was established in 2005, incorporated in 2010 and is one of over 47 IAB offices globally. IAB globally is the leading trade association for developing digital advertising technical standards and best practice.

Locally there is a financial member base of approximately 150 organisations that includes media owners, platforms, media agencies, advertising technology companies as well marketers. The board has representation from the following organisations: Carsales, Google, Guardian News & Media, Meta, News Corp Australia, Nine, REA Group, Seven West Media, Simpson Solicitors, Yahoo.

IAB Australia's charter is to grow sustainable and diverse investment in digital advertising in Australia by supporting the industry in the following ways:

- Advocacy
- Research & resources
- Education and community
- Standards

The Charter includes a focus on standards that promote trust, steps to reduce friction in the ad supply chain; and ultimately improve ad experiences for consumers, advertisers and publishers.

Executive Summary and Recommendations

- IAB Australia welcomes the opportunity to submit our views in relation to the Attorney-General's Department's *Privacy Act Review Discussion Paper* (Discussion Paper).
- IAB Australia agrees with the view expressed in the Discussion Paper that privacy laws should be fit for purpose, empower consumers, protect their data and support the digital economy.[1]
- This task requires finding the right balance between privacy obligations and a functioning digital economy, for the benefit of consumers. Consumers benefit from both privacy and engagement in the digital economy. If we get the balance between the two wrong, consumers as well as businesses and Australian society more broadly, will be disadvantaged.
- A contemporary approach to privacy regulation is required to empower consumers in the modern technological landscape. In particular, IAB supports the Discussion Paper's aim of reducing the burden of consumer consent. The burden of privacy management on individuals is too high and consent fatigue is a significant issue which undermines the goals of privacy law.
- We therefore support the approach of introducing alternative lawful grounds to consent in place of onerous privacy self-management for consumers, consistent with developments in other jurisdictions such as the UK. As the OAIC has previously stated, consent should be preserved for high privacy risk situations, rather than routine personal information handling. However, we would note it is also important not to 'throw the baby out with the bathwater' and introduce changes which have unintended consequences or simply make online business slower and less consumer friendly, for no benefit.
- IAB Australia is concerned that, taken as a whole, the proposals in the Discussion Paper would detrimentally impact on the industry's ability to function effectively. Our broad concerns are:
    - The proposed scope of information to be regulated casts the regulatory net too wide and therefore risks unintended consequences for both businesses and consumers.
    - While the proposed approach of reducing the burden of consent is important and is supported, the proposals themselves would exacerbate rather than improve the existing burden on consumers. The 'fair and reasonable' requirement, as currently framed, risks unnecessarily restricting digital advertising practices that are within consumers' expectations and not harmful.
    - The proposals go further in terms of restricting legitimate digital advertising practices than any other jurisdiction, including the EU under the GDPR. To achieve the Discussion Paper's stated objective of greater consistency with other jurisdictions,[2] if we adopt stricter GDPR style obligations, then we should also introduce GDPR style flexibilities, in particular alternative lawful bases to explicit consent.

Recommendations

- We make the following observations and recommendations in response to the specific proposals:

Scope of information regulated

- The Act should remain principles based and technology neutral as far as possible to be able to adapt to evolving technologies, business practices and consumers expectations into the future. We therefore do not support inclusion of specific technologies or digital identifiers in

[1] Privacy Act Review, Discussion Paper, 7.
[2] Discussion Paper, 8.

legislation. A more targeted approach to addressing lack of clarity in specific cases should be adopted (see section 2.2).

- The OAIC has indicated that information inferred about a person can constitute 'personal information' under the current legislation – further amendments are not required to achieve this. The Discussion Paper identifies the issue to be that it is practically difficult to determine the point at which inferences become personal information in certain circumstances. In our view, the proposal to explicitly include inferences in the scope of the legislative definition would not address this. Again, a more targeted approach to addressing any lack of clarity that exists should be adopted (see section 2.3).
- In our view, changing the term 'de-identification' to 'anonymisation' would not achieve additional clarity as the Discussion Paper suggests. We suggest a better approach would be to ensure the relevant standard required is more clearly articulated and achievable. We would support clear guidance indicating the requirement is relative to the means available to the APP entity, the amount of time required to achieve the standard and the technologies available to the APP entity at the time (see section 2.4).
- We do not support the proposal to amend the definition of sensitive information to include location information. We agree with the previous rationale of the ALRC in this regard that 'sensitive information' should not include information made sensitive by context alone. We note that the scenarios identified in the Discussion Paper regarding health information would be captured as 'sensitive information' on that basis – a change to the law is not required to achieve the same outcome in that case (see section 2.6).

Approach to consent

- While IAB Australia supports the proposed approach of reducing the burden of consent on consumers, we are concerned that the proposals in the Discussion Paper do not achieve (see section 3.1).
- The 'fair and reasonable' requirement is broad and ambiguous. It could at a minimum disrupt – or at worst be interpreted by courts to outright disallow – beneficial business uses of data, even if they are within consumers' expectations. In our view, uses such as segmentation of audiences for legitimate business purposes, data processing, audience measurement and analytics, advertising and content measurement and analytics, advertising integrity and security, market research to generate audience insights and product improvement, should not be captured as prohibited or restricted, or considered 'unfair' or 'unreasonable'. These uses should be explicitly recognised as acceptable and the privacy regulatory framework should not require businesses to provide additional notifications to consumers or seek explicit consent (see section 3.2).
- In our view, introducing a 'legitimate interests' basis for processing data may be a better way of achieving alternative lawful grounds to consent and of reducing the burden of consent on individuals. It could provide a framework for the balancing of competing interests, in a similar way as it does under the GDPR and would enable greater flexibility in relation to certain low risk, unintrusive uses within consumers' expectations (see section 3.3).

Other proposals in relation to direct marketing and pro-privacy default settings

- Requiring pro-privacy settings by default is likely to be inconsistent with consumer expectations in many cases by requiring consumers to opt-in to settings that they assume are provided as a matter of course. While we support requiring easily accessible privacy settings, we do not support a prescriptive requirement specifying how that obligation should be implemented (see sections 4.1).

- IAB supports mechanisms which assist individuals to exercise control over their personal information. However, we are concerned that any proposed right to object is framed in a manner that is practical and does not impose an unreasonable or unworkable burden on businesses. If a legitimate interests style provision is introduced, we would support a limited right to object to operate in a similar manner as it does in the UK and under GDPR. We do not support a further unqualified right to object for the purposes of direct marketing (see section 4.2).

1. Introduction

1.1 Key challenge posed by this review

This review is considering significant reforms that would, if implemented, overhaul privacy laws in Australia and impact all sectors across the economy.

There is no doubt that consumers should be more empowered and that risks in relation to privacy and confidentiality need to be appropriately mitigated. However, digital advertising and data protection are not mutually exclusive; and both serve public interests. Enhancing access to data in ways which respect consumer privacy and choice can provide social and economic benefits and enable investment in data-driven innovation.

The significant reforms being proposed need to be considered in this context. Data plays a keystone role in all online business regardless of the size and type of the business, the product and the market. The COVID pandemic and its ongoing presence and impact, has heightened the importance of businesses to evolve online. The role of data in that evolution – including with consumers – should be recognised as a key component in ensuring Australians and our economy are well placed to withstand the ongoing pandemic pressures.

This keystone role that data plays in the lives of all Australians requires lawmakers to set the right regulatory parameters to ensure individuals' privacy is protected and also ensure the smooth functioning and development of all online interactions and activities – for individuals, business and the economy. This balancing exercise is the key challenge posed by this review. The potential risks if we get it wrong are significant and are detailed further below.

While the Discussion Paper highlights the importance of this critical balancing exercise, we do not think the cumulative effect of the proposals achieves this. The proposals if implemented in their current form would risk restricting business activities, including but not limited to digital advertising that relies on data as a significant input.

Getting this balancing exercise right is no simple task and requires a framework that is flexible and adaptable. As the Discussion Paper points out, practices which may be viewed as potentially 'high risk' in one context, such as online tracking and profiling for harmful discriminatory purposes, might be beneficial in others, for example, when used for the purpose of developing services that benefit people.

This submission is focussed on the key issues for the digital advertising industry, in particular we set out our views and concerns in relation to:

- The scope of privacy regulation and the definition of personal information;
- Our views on how alternative lawful grounds to consent should be framed; and
- Our concerns in relation to other proposals that impact our industry including pro-privacy defaults, direct marketing, the right to object and new restricted practices.

1.2 Benefits of digital advertising to the economy

Online advertising, including targeted advertising, is a critical funding component of the internet ecosystem. In Australia, online advertising is produced by a highly dynamic industry that is tightly intertwined with other industry sectors that depend on and co-exist with it. For example, online advertising enables free content and services to be delivered to millions of Australians every day, fuelling the economy and enriching our lives. It also supports industry sectors across the economy including retail, finance, automotive, FMCG, technology and real estate, amongst others.

Online advertising is an essential enabler of growth for Australia's digital economy. Total Australian digital advertising expenditure reached A$11.4 billion for FY21, 24.2% growth on the previous year despite the difficulties of the pandemic.[3] Total Australian online advertising is forecast to grow at 5.5% to A$12.4billion by 2025 according to CAGR analysis by PWC for 2019 - 2025.[4]

IAB Australia, Online Advertising Expenditure Report FY21, June Quarter 2021

Digital advertising provides substantial employment and contributes to growing the nation's wealth. Individual consumers, producers and the Australian community at large derive significant benefits from the ecosystem. Digital advertising is now a significant funder of content development and will be an increasingly important revenue stream for all media companies going forward. It also sustains and promotes growth of small and medium sized businesses (SMEs) which contributes significantly to the health of the Australian economy. During the pandemic the retail sector became the top advertiser category for display advertising as online and offline retailers pivoted their businesses to suit the new environment. Addressing current and potential customers through digital advertising was vital to the survival and success of many large and small retailers.[5]

Today's digital world reflects the diversity of interests and lifestyles that characterise our society. Targeted advertising is a natural response to the evolving structure of contemporary society. It is critical to SMEs that are less able to afford to send advertising messages to consumers who are not interested in their products and services and is critical to their adaptation to increasingly digital and e-commerce driven business models.

1.3 Benefits of digital advertising to consumers

In addition to benefits to the economy, it is critical that this review not lose sight of the net public benefits that the digital advertising industry provides to consumers and Australian society at large. This fact is sometimes forgotten in debates about the most appropriate privacy laws to minimise potential harms in an online environment.

[3] IAB Australia, Online Advertising Expenditure Report FY21, June Quarter 2021.
[4] https://www.pwc.com.au/industry/entertainment-and-media-trends-analysis/outlook/internet-advertising.html
[5] IAB Australia, Online Advertising Expenditure Report FY21, June Quarter 2021.

A plethora of ad-supported services are freely available to all Australians, which increases equity of access to information as well as products and services across Australian society, strengthens communities and social networks, and promotes digital inclusion and innovation.

The Discussion Paper notes that personalised targeted advertising was the form of direct marketing of greatest concern to submitters. However, it is also important to note from the outset that these activities are not harmful per se and in fact often lead to consumer benefits such as better deals on goods and services for consumers, lower barriers to entry for small businesses and minimising consumers' exposure to irrelevant advertising. As stated in the Discussion Paper, targeted advertising has become a fundamental part of digital advertising practices that has many benefits for consumers and businesses.

A recent IPSOS survey underscored the complexity of balancing privacy interests on the one hand with ease of engagement in the digital economy on the other. It found that while consumers want organisations to respect and protect their privacy,[6] they also expect organisations to provide quality products and services,[7] as well as good customer experiences;[8] they do not want to be served too many privacy notices, and they consider advertising is the most supported model for commercial activities.[9] Other consumer surveys, including the *2020 OAIC Consumer Attitudes to Privacy Survey*, have also found that most consumers prefer ads to be relevant to them.[10] In addition, the IPSOS survey found that tracking is now 'the accepted norm'.[11]

IAB's strong view therefore is that the privacy law framework should not be framed in a way that effectively prohibits or severely restricts these activities regardless of whether or not they cause a privacy harm in the particular circumstances. To do so would ultimately be setting our privacy law framework up to fail. Responsible targeted marketing, which is reasonably expected and understood by individuals should be supported, not unnecessarily restricted. Protecting individuals from harms should not result in inhibiting responsible use of technological innovations that ultimately have the potential to benefit the industry, consumers and society more broadly.

1.4 Summary of key concerns of proposed reforms on digital advertising industry

IAB agrees with the sentiment of the Discussion Paper, in particular that the regulatory framework should:

- empower consumers, protect their data from inappropriate use and support the digital economy;
- not place overreliance on notice and consent as this may place an unrealistic burden on individuals to understand the risks of complicated information handling practices
- be consistent with privacy regimes overseas (as well as other domestic laws); and
- continue to be flexible and adaptable so that it remains relevant as new technologies and practices arise.

[6] Data Privacy, Consumer Perceptions of Data Privacy and the value of commercial exchange, October 2021, 7. Prepared by IPSOS for presentation to IAB Measure-up Conference.

[7] Ibid, 10.

[8] Ibid, 10.

[9] Ibid, 22.

[10] 2020 OAIC Community Attitudes to Privacy Survey.

[11] Ibid, 14.

However, we are concerned that the proposals, particularly when viewed collectively, do not achieve this. Specifically, we have the following three overarching concerns arising out of the Discussion Paper:

1. The proposed scope of information to be regulated is too broad and risks significant unintended consequences for digital advertising, businesses and consumers.

In our view, proposed changes to the definition of personal information and the consequent scope of privacy regulation being proposed, poses risks for the digital advertising industry, businesses and consumers. Broadly, we are concerned this would:

- increase the complexity of technical information that needs to be disclosed by businesses to consumers, potentially giving rise to a huge administrative burden on organisations;
- place increased stress on consumer understanding of privacy policies and notices – which would be contrary to the goals of this review;
- introduce technology specific changes that will date quickly; and
- stifle innovation.

These risks are significant and raise an important question in relation to whether, if there are harms to be addressed, privacy laws are the most appropriate regulatory tool to address those harms. In IAB's view, more targeted regulatory tools which prevent harms based on differential treatment, such as discrimination laws, consumer protection laws, regulations that address the targeting of children, tracking and surveillance, disinformation and misinformation, may be more appropriate in relation to harms that arise regardless of whether a natural person is reasonably identifiable. We note that some examples of harms provided in the Discussion Paper are already covered by existing laws and we address this further below.

In addition, we are concerned that the regulatory framework should remain technology neutral. This aspect of the existing framework has been a success and meant that the law has adapted in many ways to new technologies that have developed over time.

2. The 'fair and reasonable' requirement, as currently framed, would restrict digital advertising practices that are within consumers' expectations, are not harmful and that are important to the industry functioning.

Digital advertising relies on the collection of data. While IAB supports introducing alternative lawful grounds to consent, we are concerned that the proposed 'fair and reasonable' requirement as framed would:

- at a minimum disrupt – or at worst be interpreted by courts to outright disallow – beneficial business uses of data, even if they are within consumers' expectations. For example, segmentation of audiences is an accepted advertising practice, but it would be unclear whether this would automatically be considered unfair;
- apply in addition to consumer consent requirements, rather than as an alternative ground to consent, therefore increasing the burden on APP entities but doing nothing to reduce the burden on consumers; and
- operate regardless of whether or not a consumer has consented (unlike the EU legitimate interests ground), therefore taking away consumer choice, contrary to the goals stated in the Discussion Paper.

In our view, consideration should be given to whether the introduction of a legitimate interests ground would better achieve the goal of reducing the burden on consumer consent requirements stated in

the Discussion Paper. Either way, if we adopt stricter GDPR style obligations, then we should also introduce GDPR style flexibilities, in particular alternative lawful bases to explicit consent.

3. The proposals taken together go further in terms of restricting legitimate digital advertising practices than any other jurisdiction, including the EU under the GDPR, and this would have a negative impact on Australian businesses, businesses seeking to enter the Australian market and innovation.

The proposals would not achieve international consistency, a goal noted as important in the Discussion Paper. Rather, it would put Australian businesses at a competitive disadvantage to those based overseas. Unlike jurisdictions such as the UK and EU, the proposals would increase the scope of regulation and place additional restrictions on how that broader scope of information may be used. As stated above, while proposing to introduce additional restrictions from both the EU and Canada regulatory frameworks, nothing in the proposals would introduce the flexibilities that exist in those jurisdictions for legitimate business uses that are not harmful.

The likely net cumulative effect of this approach is alarming at best. It would inhibit data flows that sustain business products and services, diminishing the utility and value of these products and services which benefit consumers in the global digital economy. Products and services already compliant with current law and that rely on data availability would be substantially curtailed. This impact would be disproportionately borne by SMEs that are least able to do so.

2. Scope of privacy regulation and definition of Personal Information

As noted in the Discussion Paper, the definitions of 'personal information' and 'de-identified' determine the scope of the Act. Information that falls within the definition of 'personal information' must be handled in accordance with the Act.

In the context of digital advertising, the issue of whether differentiated information should fall under the definition of 'personal information' has been raised. As indicated in our responses to the specific proposals below, we do not consider that data which does not reasonably identify an individual should be defined as 'personal information'. Generally speaking, privacy harms arise at the point of identification of a natural person. Most data required for digital advertising is not data that would reasonably identify any person and in our view should therefore not be subject to privacy laws.

However, as discussed below:

- clarification may be required in relation to the point at which information, including inferred information, is reasonably identifiable, particularly in the context of modern data practices; and

- further consideration may need to be given to the best way to address harms that may arise from certain uses of differentiated information which is not 'personal information' and where there is a low risk of individuals being identified.

In relation to the first point, in our view, the Discussion Paper raises the issue of clarifying the point at which information becomes 'reasonably identifiable' in the context of modern data practices however we do not think that any of the proposals would effectively provide clarity on this. We detail why below.

In relation to the second point, this should be addressed through the most appropriate laws to deal with these harms, for example, dynamic pricing practices may be better dealt with under existing competition and consumers laws.

We address the specific proposals in relation to the definition of 'personal information' below.

2.1 Proposed changes to the existing definition

The Privacy Act currently defines 'personal information' as:

> *'Information or an opinion about an identified individual, or an individual who is reasonably identifiable:*
>
> *a) Whether the information or opinion is true or not; and*
> *b) Whether the information or opinion is recorded in a material form or not.'*

The Discussion Paper proposes that the definition should be amended as follows:[12]

- change the word 'about' in the definition of personal information to 'relates to';
- include a non-exhaustive list of the types of information capable of being covered by the definition of personal information;

[12] Discussion Paper, Proposal 2.

- 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;
- amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information; and
- require personal information to be anonymous (rather than "de-identified") before it is no longer protected by the Act.

We address these proposals below.

2.2 Clarifying the position with respect to technical information

As indicated in the Discussion Paper the proposed changes are intended to clarify the position with respect to technical information, particularly in the context of the decision in *Privacy Commissioner v Telstra Corporation Ltd 2017 FCAFC 4* (Grubb):

> *"..the Act's application to technical information became uncertain following the decision in Privacy Commissioner v Telstra Corporation Ltd 2017 FCAFC 4 (Grubb). There it was held that an individual must be the subject matter of the information for it to be 'about an individual' and within the scope of the Act. This was found to involve an evaluative conclusion depending on the facts of the case, to be assessed alone or in conjunction with other available information. This approach raises difficulties for APP entities that may not feel confident in assessing if information is 'about an individual'. Without greater legal clarity as to the meaning of the phrase, APP entities may contend that technical information is not 'about an individual', rather than 'err[ing] on the side of caution' as per the OAIC Guidelines."*[13]

As the Discussion Paper states, the law itself is not unclear. Data on its own that does not identify an individual is not considered to be 'personal information'. However, where a digital identifier is used in a manner that does identify a person (for example, when stored with or linked to other personal information that identifies a person, such as where an individual logs into their online account), then it will be considered 'personal information' at that point.

In recommending the existing definition, the ALRC noted that the definition remain 'sufficiently flexible and technology-neutral to encompass changes in the way that information that identifies an individual is collected and handled'. As the Issues Paper to this Review Paper quite rightly pointed out, 'identifiability' captures a broader range of information than 'identity', including some online identifiers – if and when they are about a natural person.[14]

However, what may be unclear is how the definition applies to digital identifiers, potentially leading to confusion by some APP entities, for example the Discussion Paper raises the scenario of a number of digital identifiers being used together (IP address, device identifier and location data) in a manner that enables identification of an individual;[15]or circumstances where secondary or indirect identifiers derived from primary identifiers may identify an individual.

As the law already includes the requirement that personal information be associated with an individual that is "identified or reasonably identifiable", examples such as these may benefit from clarification in relation to the point at which an individual is either identifiable or reasonably identifiable.

---

[13] Discussion Paper, 21.

[14] Privacy Act Review, Issues Paper, October 2020.

[15] Discussion Paper, 22.

While clarification is welcome, IAB does not support moving away from the technology neutral approach currently adopted in legislation, as any scenarios included would not be comprehensive and may date relatively quickly, giving rise to further uncertainty about any identifiers not included.

In addition, in relation to identifiers that were specifically included, it may also create further confusion, because, as identified both in the Grubb case and by the OAIC, it would depend on the specific circumstances in which the digital identifiers were used and whether those circumstances allowed an individual to be 'reasonably identifiable'.[16]

IAB would therefore consider that it may be more useful for APP entities if the OAIC gave guidance, not only in relation to the types of identifiers that may constitute personal information, but also, provide examples of the circumstances where that would be likely be the case. Any clarification would also need to be acknowledged as limited and dependent on the circumstances of the data collection and use. While a list of objective factors may assist APP entities to make an assessment about 'reasonable identifiability', any assessment will necessarily depend on an assessment of the relevant technology.

2.3 Inferred information

The Discussion Paper proposes to amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information. It provides that the new definition will cover circumstances 'where an APP entity infers, derives, generates or otherwise creates personal information, whether or not this is done by or on behalf of an individual'.[17]

As noted in the Discussion Paper however:

> *"Inferred information will meet the definition of 'personal information' if it is 'about an identified individual, or an individual who is reasonably identifiable'. The definition of personal information already contemplates inferences by seeking to cover 'opinions', 'whether true or not' about an individual. However, APP entities may find it difficult to practically determine the point at which the opinions or inferences they generate become personal information."*[18]

We think the Discussion Paper correctly identifies the issue with inferred information being that it may be practically difficult to determine the point at which inferences become personal information in certain circumstances, for example, data analytics – at what point in the process of analysing a large variety of non-identifying information, does a person becomes reasonably identifiable? Is this technology dependent?

However, we would caution that changing the definition as proposed will not change the practical difficulty in determining at what point an inference will be 'personal information'. We note that European data protection law has similarly been criticised as 'failing in this regard', with some experts noting that individuals need to 'consult sectoral laws and governing bodies applicable to their specific case to seek possible recourse'.[19]

We therefore consider that a more targeted approach to the problem might be to provide guidance to APP entities in relation to the various contexts in which it is unclear whether or not inferences constitute personal information and/or the types of uses that would not be within the reasonable expectations of consumers (though, as indicated above, any guidance would be dependent on the

---

[16] *Privacy Commissioner v Telstra Corporation Limited [2017]* FCAFC 4.

[17] Discussion Paper, 28.

[18] Discussion Paper, 24.

[19] https://www.law.ox.ac.uk/business-law-blog/blog/2018/10/right-reasonable-inferences-re-thinking-data-protection-law-age-big

particular circumstances and need to be updated reasonably regularly given that both technologies and consumers' expectations with respect to privacy are constantly changing).[20]

We note that the Discussion identified targeted advertising as a practice of particular consumer concern,[21] and the proposal in relation to inferred information is intended to address this concern.

The Discussion Paper also raises concerns in relation to harm that may be caused even where a person is not 'reasonably identifiable' in relation to some practices which are unfair.

Where a person is not reasonably identifiable, in our view the proportionate response to targeting generally is to require organisations to provide individuals with clear and easily accessible opt-out rights (see section 4.1 below).

While this proposal will not assist to determine the point is an inference drawn, or necessarily provide any additional protection to consumers in relation to inferences, it risks:

- Significantly increasing compliance obligations for organisations or potentially require organisations to substantially redesign existing systems that operate globally;
- Introducing confusion in relation to the point at which privacy obligations for organisations arise (for example, notice & consent requirements)
- having a chilling effect on use of artificial intelligence and machine learning in Australia for these reasons.

2.4 Anonymisation

The Discussion Paper proposes to require that personal information be anonymous, rather than de-identified, before it is no longer protected by the Act. The Discussion Paper notes that the word 'anonymous' could more clearly signal to APP entities that they are required to meet 'the higher, irreversible standard reflected by the term', and that 'information would be considered 'anonymous' if it were no longer possible to identify someone from the information.[22]

IAB is not convinced that simply changing the terminology would achieve clarity as the Discussion Paper suggests and is therefore not supportive of this proposal. Specifically, we are concerned:

- it is unclear what this proposal would mean in practice. As information that is de-identified is not 'personal information', it is unclear how the Privacy Act would apply to de-identified information (which by definition, means that a natural person is not 'reasonably identifiable'); and
- 'anonymisation', particularly as framed in the Discussion Paper, would be an unachievable standard and would discourage the sharing of information with third parties for research and other beneficial purposes, and using service providers to process data on an entity's behalf, even where the risk of re-identification was very low or negligible or where consent has been obtained.

De-identification currently requires that information has undergone a process whereby the risk of an individual being re-identified in the data is very low in the relevant context. The OAIC defines this as requiring that 'there is no reasonable likelihood of re-identification occurring'. In practice, as the OAIC points out, it requires:[23]

- The removal of direct identifiers; and either

[20] IPSOS research/ OAIC 2020 Australian Community Attitudes to Privacy Survey research

[21] Discussion Paper, 21.

[22] Discussion Paper, 30-31.

[23] https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act#:~:text=Information%20will%20be%20de%2Didentified,likelihood%20of%20re%2Didentification%20occurring.

- Removing or altering other information that could potentially be used to re-identify an individual; and/or
- The use of controls and safeguards in the data access environment to prevent re-identification.

IAB considers this a high standard if implemented appropriately in the circumstances, and is used extensively by APP entities wishing for their data service providers to process their data in a secure manner.

The Discussion Paper provides that anonymisation is the process of irreversibly treating data so that no individual can be identified, including by the holders of the data.[24] IAB is concerned that this is not an achievable standard. Whether data can be re-identified is context and technology dependent. It is not possible to ensure that technologies and circumstances will not evolve to enable re-identification.

IAB therefore considers a better approach would be to ensure the relevant standard that is required is high but not unachievable and that it is well understood by APP entities in the context of evolving technologies and data processes. The standard to be applied before data is considered to fall outside the scope of privacy laws is currently under review in other jurisdictions, for example:

- The UK is looking at confirmation in legislation that 'anonymisation' needs to be relative to the means available to the data controller and that there needs to be recognition that compliance can change over time and is dependent on the circumstances of the particular entity.[25]

- In Canada, lawmakers are proposing to consider factors like costs and the amount of time required for identification and available technologies.[26]

The proposal would also render much legitimate data processing unviable, or even increase risk to consumers if APP entities which currently de-identify personal information before sending it to their service providers choose to provide open and identifiable personal information to their service providers instead. This is a risk if anonymised data is not of any use to the controller, once the service provider had performed their task. This could have the effect of increasing the risk of a data breach in the hands of the service provider – which would be a perverse outcome.

In our view, the standard adopted needs to be achievable and in alignment with international definitions which recognise the difficulties in achieving both an acceptable standard of de-identification/anonymisation on the one hand, but also a practical, clear and certain definition which is workable for businesses on the other. We would support incorporating in legislation or guidance material, clear guidance that the standard adopted is relative to the means available to the APP entity, the amount of time required for re-identification and technologies available at the time.

2.5 At what point is a person 'reasonably identifiable'?

The Discussion Paper proposes to define 'reasonably identifiable' to cover circumstances in which an individual could be identified directly or indirectly and to include a list of factors to support this assessment. [27]

[24] Discussion Paper, 30.

[25] ICO report

[26] Ibid; CPPA: Identifying The Inscrutable Meaning And Policy Behind The De-identifying Provisions - Privacy - Canada (mondaq.com)

[27] Discussion Paper, 28.

IAB Australia does not consider it necessary to further define 'reasonably identifiable' in legislation. The proposal to include the words 'directly or indirectly' would not change the current understanding or interpretation of 'reasonably identifiable', particularly given the OAIC APP guidelines currently make clear that other available information should also be considered when determining the risk of someone being identified.[28]

In addition, the OAIC APP guidelines already provide a list of factors that should be taken into consideration in determining whether an individual is reasonably identifiable. However, there is merit in providing updated guidance in relation to how to determine when an individual is 'reasonably identifiable' in practice. Factors such as costs, the amount of time required for identification and the technologies available to the particular APP entity should be taken into consideration when determining whether someone is reasonably identifiable in the particular circumstances.

2.6 Definition of sensitive information

The Discussion Paper seeks feedback on whether the definition of sensitive information in section 6(1) of the Act should expanded to incorporate various updates in the EU as well as various other types of information. One of the types of information the Discussion Paper raises is location information. We do not support the inclusion of location information in the definition of sensitive information, for the same reasons set out above – we do not support increasing the consent burden on consumers. In addition, as noted above, a recent IPSOS Consumer Survey found that tracking is an area where consumer attitudes are changing.

While use of location information may be intrusive in certain circumstances, for example if it reveals other sensitive attributes about a person, it is not the location data that is sensitive per se, it is the sensitive information that comes to light as a result. In fact, location data of itself is not even personal information under the current Act (notwithstanding it can provide useful audience insights to a collector), yet this proposal is attempting to take it from being non-personal information, not only to personal information, but further, to sensitive personal information. In our view, this would not be a reasonable outcome.

It is the case with any personal information that it can become more or less sensitive depending on the context in which it is considered. The ALRC considered this issue in its report, *'For your information: Australian Privacy Law and Practice'*, and considered that the definition of 'sensitive information' should therefore not include information made sensitive by context, because of the very stringent requirements that are imposed as a result. We agree.

In addition, in the scenario raised in the Discussion Paper where location data reveals that a person has visited an HIV clinic, that information would already captured under current law as 'sensitive' if it can be linked to a reasonably identifiable person, because it is health information. Similarly, if a person purchases a specific type of medication online, there is unlikely to be any harm caused if they are not 'reasonably identifiable', and if they are 'reasonably identifiable', then this would again fall within the definition of health information which is already classed as sensitive. In cases where location data is used for nefarious purposes, other laws may also apply, such as surveillance devices legislation and other criminal provisions that are directly targeted at behaviours such as stalking and harassment.

In the large percentage of cases where location information is used for ordinary business purposes, for example, providing a customer with more relevant search results, the law should not be changed to require additional disclosure obligations or consumer consent requirements.

[28] APP guidelines, p 20.

2.7 Cumulative impact

IAB is concerned to ensure that any broadening of the definition of or concepts around what is personal information needs to be critically and practically assessed in the context of the other proposed reforms (for example, the proposed 'fair and reasonable' requirement), to measure the likely cumulative impact overall. The result in some cases would be entirely unworkable and bring some services, let alone the consumers using those services, to their knees with the pure volume and frequency of disclosures to be made and consents obtained. It is simply not pragmatic.

3. Alternative lawful grounds to consent

3.1 The approach of reducing the burden of consent is supported

The Discussion Paper proposes that a collection, use or disclosure of personal information under APP 3 or APP 6 must be fair and reasonable in the circumstances.[29]

It notes that, "Currently, the protections within the APPs rely predominantly on a regulatory theory of privacy self-management", in that APP entities are required to notify individuals of the specific purposes for which their information will be handled. The responsibility is then on the individual to consider the costs and benefits of providing the information and engage with APP entities as they wish.[30]

As noted in the Discussion Paper, a number of submitters to the Issues Paper argued that there are limitations with this, for example, it is becoming increasingly difficult for individuals to assess privacy risks, particularly in the context that 'there are too many entities collecting and using personal data to make it feasible for people to manage their privacy separately with each entity'.[31]

In its submission to the Issues Paper, the OAIC stated that:

> *"the burden of understanding and consenting to complicated practices should not fall on individuals…"*

In the same submission, the OAIC also recommended that consent should be preserved '*..for high privacy risk situations, rather than routine personal information handling*'.

The approach of developing alternative lawful grounds to consent is also increasingly being adopted in other jurisdictions. In the UK for example, the *Data: A new direction* consultation paper provides:

> "*The UK has been a strong proponent of alternative lawful grounds to consent, recognising that there are a number of common scenarios where it may be appropriate to process personal data without seeking consent. This could be the case, for example, where it would be very difficult or inappropriate to seek the individual's consent, or where a low-risk processing activity is being undertaken without consent, but in line with an individual's expectations*."[32]

We understand that other jurisdictions also take this approach, for example Singapore's law also defines various types of processing activity to be in the 'legitimate interests' of the data controller.[33]

IAB Australia acknowledges and agrees that the burden of privacy management on individuals is too high and an alternative approach is needed. Consent fatigue is a significant issue which undermines the goals of privacy law. We therefore support the approach of introducing alternative lawful grounds to consent in place of onerous privacy self-management for consumers.

The Discussion Paper indicates that two options were considered to achieve such as approach:

1. A lawful basis for collection, use and disclosure modelled on the 'legitimate interest' test under Article 6(1)(f) of the GDPR; or

[29] Discussion Paper, proposal 10.1.
[30] Discussion Paper, 80 - 82.
[31] Ibid, 82
[32] Data: A new direction, paragraph 55, p 21.
[33] Ibid, 22. See also https://sso.agc.gov.sg/SL-Supp/S63-2021/Published/20210129?DocDate=20210129

2. A general requirement that entities do not undertake acts or practices in relation to an individual's personal information that would be unfair, cause harm, or be outside the reasonable expectations of an ordinary individual.[34]

The Discussion Paper ultimately proposes a 'fair and reasonable' requirement in conjunction with various legislated factors to assist entities in determining whether a particular collection use or disclosure is acceptable.

While we agree with the broad approach of introducing alternative lawful grounds to consent, we do not support the 'fair and reasonable' proposal as framed. We also do not agree with the reasons provided in the Discussion Paper for not adopting a legitimate interests basis under Australian law. We outline our reasoning in relation to these two options below.

3.2 'Fair and reasonable' requirement not supported as currently framed

The proposed fair and reasonable requirement is too broad and on our reading would, if implemented, effectively prevent digital advertising activities that are within consumer expectations and that are important to the digital economy functioning. We note the following concerns:

- The test as framed would result in significant uncertainty in relation to legitimate business activities and whether they would be compliant or not. It would be a perverse outcome of this review if uses which may be within a consumer's expectations, have become acceptable business practice and do not cause any harm were no longer permitted.

- Assessing what is 'fair and reasonable' or within 'community expectations' is extremely difficult when it comes to privacy. As the Discussion Paper notes,
    - Technologies and data practices are constantly changing
    - Privacy risks are constantly emerging and evolving
    - Social norms are constantly changing
    - Individual expectations of privacy are highly varied and variable over time

  These factors exacerbate the uncertainty inherent in a 'fair and reasonable' requirement for business.

- The Discussion Paper provides that 'Similar fairness-based protections can be found in other Commonwealth legislation, for example, the unfair terms regime in the ACL'. However, the requirement as framed in the proposals is much broader than the requirement to 'deal on fair terms' which exists under consumer law. [35]

- The test appears to be proposed to apply in addition to consumer consent requirements, rather than as an alternative ground to consent. Therefore, while it would increase the burden on APP entities, it would do nothing to reduce the burden on consumers.

For these reasons, we do not support the 'fair and reasonable' test as currently framed. In our view, uses such as segmentation of audiences for legitimate business purposes, data processing, audience measurement and analytics, advertising and content measurement and analytics, advertising integrity and security, market research to generate audience insights and product improvement and frequency capping and innovation, should not be captured as prohibited or restricted, or considered 'unfair' or

[34] Discussion Paper, 83.

[35] For example, see https://consumer.gov.au/sites/consumer/files/2016/05/0553FT_ACL-guides_ContractTerms_web.pdf

'unreasonable'. These uses should be explicitly recognised as acceptable, and the privacy regulatory framework should not require businesses to provide additional notifications to consumers, seek additional consents simply because the manner in which these legitimate activities are undertaken has changed, or make further assessments about fairness or reasonableness, so long as consumers are notified of these purposes at the point of collection.

3.3 'Legitimate interests' basis for processing data favoured

As noted in the Discussion Paper, many industry stakeholders raised the GDPR's legitimate interest basis for processing personal data as a desirable basis for the handling of personal information in Australia.

In our view, introduction of a legitimate interests basis for processing data may be a better way of achieving alternative lawful grounds to consent and of reducing the burden of consent on individuals. This is because, it could provide a framework for the balancing of competing interests, in a similar way as it does under the GDPR.

As noted in the paper, the GDPR provides six lawful bases for processing data, namely: [36]

1. consent;
2. performance of a contract;
3. compliance with a legal obligation;
4. protecting the vital interests of a person;
5. performance of a task in the public interest or in the exercise of official authority; and
6. legitimate interests of the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

The sixth 'legitimate interests' basis is seen as different to the other lawful bases as it is not purpose-based (unlike 2 to 5). It is more flexible and 'could in principle apply to any type of processing for any reasonable purpose'.[37]

In Australia on the other hand, personal information can only be collected where the information is reasonably necessary for, or directly related to, one or more of an organisation's functions or activities. In addition, an organisation may only collect sensitive information if the individual consents, unless an exception applies (including for example, lessening or preventing a serious threat to life, health or safety, taking appropriate action in relation to suspected unlawful activity or serious misconduct, reasonably necessary for establishing, exercising or defending a legal or equitable clam).[38]

In addition, an organisation can only use or disclose the Personal Information for a purpose for which it was collected or for a secondary purpose in certain limited circumstances. However, we do not have equivalent flexible bases as exist under the GDPR which enable legitimate or public interest uses of personal information without consent. Under the proposals in the Discussion Paper, the regulatory framework in Australia would become even more restrictive as the use would also have to pass the proposed new fair and reasonable test.

In our view, the introduction of a legitimate interests ground would enable a similar balancing of rights as 'legitimate interests' provides in the EU, and would go towards achieving the goals stated in the Discussion Paper, and which the OAIC has also called for, of reducing the burden on consumer consent requirements. It would introduce flexibilities in relation to certain low-risk non-purpose-based uses which are unintrusive and within consumers' expectations.

---

[36] Article 29 Working Party (FN 501)

[37] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/

[38] APP 3.4.

However, the Discussion Paper ultimately does not propose a legitimate interests basis for processing data be introduced. It notes:

> "*As the Act does not confer a right to privacy on individuals, but rather protects against arbitrary interference with privacy as derived from Article 17 of the ICCPR, it may present difficulties to import a rights-based requirement*."[39]

We do not agree with this reasoning. While there is no 'right to privacy' per se in Australia, such as a tort of invasion of privacy, the Privacy Act does confer a range of protections with respect to information privacy on individuals. As the Discussion Paper points out, this right derives from the ICCPR which protects privacy as a fundamental human right. While these rights are not absolute, they are protected and balanced against other rights such as the public interest. This is not dissimilar to the approach adopted in the GDPR where privacy is also balanced against a range or competing rights, which are specifically referred to in Article 6.

The fact that information privacy rights are not absolute and must be balanced against competing rights is already acknowledged in the Privacy Act, for example:

- The Act provides that amongst its objects are "to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities";
- The Act deems various practices of organisations not to constitute an interference with privacy; and
- The Act contains various provisions which require balancing against the safety of individuals or with compliance with the law.

We therefore consider that inclusion of a 'legitimate interests' style ground would be consistent with the existing approach taken in the Privacy Act, and with international approaches as well.

Regardless of the approach we take, we think the outcome should be additional flexibility in relation to uses which are low risk, unintrusive and related to data processing and other legitimate business interests, to enable APP entities to collect, use or disclose personal information without consumer consent in clear circumstances. This would then reserve consent for those collections, uses and disclosures that are out of the ordinary and fall outside of a consumer's expectations. It would also assist to reduce consent fatigue.

3.4 Proposal to define consent

Proposal 9.1 in the Discussion Paper proposes that consent be defined in the Act as being 'voluntary, informed, current, specific and an unambiguous indication through clear action'.

We do not think this proposal adds much given the APP Guidelines already require consent to be voluntary, informed, current and specific.[40] In addition, we do not support the inclusion of 'unambiguous' in legislation or the Guidelines as a requirement for consent. The Discussion Paper notes that consent would need to be opt-in to be 'unambiguous' which we do not support for the reasons outlined in section 4.1 below. In our view, an opt-in approach would result in significantly higher costs on consumers, businesses and the economy.

While IAB Australia supports the Discussion Paper's statements in relation to reducing the burden on consumer consent, we think that inclusion of 'unambiguous', if taken to require 'opt-in' consent, would have the opposite effect and in fact increase the burden of consent and lead to increased

[39] Discussion Paper, 83.

[40] APP Guidelines, https://www.oaic.gov.au/__data/assets/pdf_file/0009/1125/app-guidelines-july-2019.pdf

consent fatigue. We favour an approach of enabling businesses to consider the most effective way to obtain consent in the context of their businesses and the design of their customer interfaces.

4. Other specific proposals

4.1 Pro-privacy default settings

The Discussion Paper proposes to introduce pro-privacy defaults on a sector or other specified basis and provides two options:

1. Pro-privacy settings enabled by default – i.e. an entity must pre-select the most restrictive privacy settings when it offers a product or service that contains multiple levels of privacy settings;
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.

IAB does not support the pro-privacy default settings in the form proposed in the Discussion Paper.

In relation to the first option, we think this is likely to be inconsistent with consumer expectations in many cases and could therefore negatively impact on consumer experiences and a business' ability to ensure they can provide a smooth and efficient service to an individual consistent with those expectations. A recent IPSOS survey showed that consumers do not want to be subject to onerous consent requests or processes that slow-down their online experience.[41] As outlined above, we would strongly advise against introducing any regulations or requirements which are likely to increase consent fatigue.

In addition, IAB notes that a study on the negative effects of opt-in rules under the *Privacy and Electronic Communications Directive (2002/58/EC)* found that, after the EU's opt-in regulation came into effect, the result was an average reduction in the effectiveness of online ads by approximately 65 percent. This reduced the available funding for online companies and their capacity to innovate, and lowered functionality for consumers. The study concluded that this is an important reason for the relatively fewer number of internet start-ups in Europe compared with the United States, as they have a harder time funding their businesses.[42]

In relation to the second option, we support requiring easily accessible privacy settings and ensuring that entities are required to provide individuals with a clear way to set their privacy controls and opt-out of practices such as targeted advertising if they want to, consistent with their preferences and expectations. However, we do not support any new requirement specifying how that obligation should be implemented. It should be a matter for APP entities to determine the most appropriate way to implement this requirement, in the context of the operation of their online businesses. Mandating a specific way to implement this requirement is unnecessary and could negatively impact some business models, for example, if the manner mandated is not consistent or easily able to be integrated with business systems and user interfaces.

4.2 Right to object and direct marketing

The Discussion Paper proposes to introduce a right to object whereby an individual may object or withdraw their consent at any time, and upon receiving notice of an objection, an entity must take

[41] IPSOS survey, slide 12. See https://iabaustralia.com.au/resource/digital-data-exchange-the-consumer-view/

[42] ITIF, The Negative Effects of Opt-In Rules; see https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules)

reasonable steps to stop collecting, using or disclosing the individual's personal information and must inform the individual of the consequences of the objection.

IAB broadly supports mechanisms which assist individuals to exercise control over their personal information. However, the proposed right to object needs to be designed carefully so that it does not have unintended consequences. IAB is concerned, firstly that, as identified in the Discussion Paper, if a consumer objects to their data being collected for an intrinsic part of a service, it should be possible for companies to no longer offer the service. This includes instances where products have ad-supported business models. This should be clarified explicitly and is essential for the businesses to be able to practically implement this proposal.

Secondly, the proposed right to object as currently framed in the Discussion Paper, goes further than the similar right established under the GDPR.[43] Under the GDPR, it can only be exercised when the legal basis for processing data is permitted under 'legitimate interests' or 'public interest' bases. In addition, the right to object is essentially required to be weighed up against other factors including freedom of speech and the rights of media organisations to publish in the public interest. In our view, this approach is more balanced than the proposal in the Discussion Paper. If a legitimate interests style provision was introduced as discussed above, a right to object could be introduced to operate in a similar manner as it does in the EU and UK.

In addition to the general right to object, the Discussion Paper also proposes an unqualified right to object to the collection, use and disclosure of personal information for the purposes of direct marketing. For direct marketing, the Discussion Paper provides that, an organisation must notify the individual of their right to object in relation to each marketing product provided and upon receiving notice of an objection, an entity must stop collecting, using and disclosing the personal information. In our view, this additional and unqualified right is not required. If a general right to object is introduced, it could apply regardless of the purpose of the collection, use or disclosure of the personal information.

It would be even more concerning if the right to object compelled advertising providers to fundamentally change their business models in response to a consumer exercising this right. As outlined earlier, targeted advertising brings enormous economic benefits to small businesses and Australian consumers. It appears that the review may be contemplating a right to object that would compel ad-supported services to continue providing those services without ads. Given the wide array of entertainment, news and digital services that are available, if a consumer fundamentally objects to the ad-supported business model of those services, they are easily able to shift to another service instead.

4.3 New restricted practices

The Discussion Paper proposes that certain practices be determined to be 'restricted practices' with the consequence that either:

1. APP entities must take reasonable steps to identify privacy risks and implement measures to mitigate those risks; or
2. APP entities increase an individual's capacity to self-manage their privacy in relation to the restricted practice.

The paper proposes that restricted practices include, amongst others, direct marketing including online targeted advertising on a large scale.

[43] See Article 21, GDPR.

IAB's view currently is that we do not have sufficient information to support the proposal and that the issues raised by these practices can be dealt with under other general heads of the Act. We have already seen how calling out specific practices (such as direct marketing) can become quickly dated and the temptation to do so again should be avoided. It can only result in short term clarity followed by long term confusion and/ or redundancy as technology and practices change.

In relation to the first option, all APP entities are already required to take reasonable steps to identify privacy risks and implement measures to mitigate those risks. APP 1 provides that APP entities 'must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's function or activities that: will ensure the entity complies with the APPs and a registered APP Code that binds the entity; and will enable the entity to deal with inquiries or complaints.. about the entity's compliance..'. It is therefore unclear how Option 1 would be any different to what is currently required of all APP entities.[44]

In relation to Option 2, this is also a little unclear. While we broadly support transparency and consumer choice, absolute opt-out rights are exercised at the point of engaging with a particular service. In relation to the suggestion of additional notice or consent requirements, we would not be supportive of this approach. Our approach to consent is set out in detail in section 3 above.

[44] APP 1.2(a)-(b)

5. Conclusion

IAB Australia thanks the Attorney-General's Department for the opportunity to make this submission.

Our members strongly support fit for purpose privacy laws that empower consumers, protect their data from misuse and support the digital economy. This will also support the Government's *Data Strategy* aims for Australia to be a leading digital economy and society, and for all Australian businesses to be digital businesses by 2030.[45]

We look forward to working with the Government to ensure the right balance between privacy obligations and a functioning digital economy can be achieved.

[45] https://ausdatastrategy.pmc.gov.au/sites/default/files/2021-12/australian-data-strategy.pdf