Submission to the

Australian Government's

Privacy Act Review Report Consultation

on behalf of

The Media Federation of Australia

6 April 2023

The Media Federation of Australia welcomes the opportunity to make a submission to the Privacy Act Review Report 2022 (Report) to assist in informing the Australian Government's response to the Report as part of the consultation process.

About the Media Federation of Australia (MFA)

The Media Federation of Australia (MFA) represents media agencies providing services to advertisers across all media channels, including media planning and buying, proprietary systems and tools, data and analytics, and content development. The MFA's members account for over 90 percent of all media billings placed by media agencies in Australia.

The media agency sector comprises a diverse range of firms, including highly specialised agencies and full-scale agencies offering a comprehensive suite of advertising and media services. MFA's members include the local offices of all the major media agency networks including Omnicom Media Group, GroupM, Dentsu, Publicis Media, IPG Mediabrands and Havas Media, as well as Australian independent agencies such as Slingshot, Atomic 212 and Pearman Media. A full list of MFA members can be found here.

As an alliance of media agencies, the MFA's charter is to:

- Represent and advocate for the industry;
- Set best practice standards and guidelines; and
- Provide skills and best practice training for our members.

The MFA aims to share its deep and practical knowledge of the media and advertising industry to bring a deeper understanding into the discussions on privacy reforms in Australia. The MFA has also consulted with its membership base and other industry participants across the media industry on the Report and aims to identify and voice some of these key concerns and illustrate the practical implications with a number of the Report proposals.

Executive Summary

The MFA supports the modernisation of our privacy laws that protects consumers, and allows for our media industry, local business, and digital economy to function, innovate and prosper. Privacy reforms should retain flexibility for business to tailor their compliance measures to specific risks and use cases. Our privacy laws should aim to be future proof, provide businesses clear lawful bases for the use and processing of data, and allow responses to new and emerging conditions.

Business practices in digital advertising and the use of data are rapidly evolving and being driven by innovation and technological developments in the industry. In response to the evolution in data privacy considerations and regulation, industry participants are already developing new privacy focussed practices and safeguards. These include:

- the use of 'Data Clean Rooms' a privacy safe method of analysing data without identifiers being shared, in a secure environment. This involves the matching of data sets by a third party anonymously and with strict data access limitations. In practice this is two or more entities matching their data in a neutral zone using a third party platform or a piece of software. The third party platform or software encrypts the data set so that it is not possible to extrapolate the data back. The data sets are then 'joined' to provide scale and insight. An example is an advertiser matching their data with Channel 7 data to understand what the advertiser's customers are viewing, how many of them are viewing and what they are doing; and
- organisations are increasingly using modelled audience data also known as 'lookalikes' / anonymised data rather than personal information.

There are many consumer and community benefits in a thriving and innovative advertising and media industry and digital economy. Digital advertising plays a central role in Australia's economy and provides significant value to the Australian economy, consumers, and society. Digital advertising:

- contributed $13 billion of direct revenue in 2021 to the Australian economy;
- contributed $94 billion in direct and flow-on contribution to Australia's national income (as measured by gross domestic product or GDP) in 2021;[1]
- enables the delivery of free online content, products and services to all Australians, grows businesses, and supports 450,000 jobs (24,600 directly);
- contributed $55.5 billion in total annual consumer benefits for the Australian community in 2021, consisting of:
  - $8.8 billion value from access to free ad-supported digital services and content;
  - $10.2 billion value from consumption being more closely matched to consumer preferences; and
  - $36.5 billion decreased transaction costs via reduced time and cost savings.

The ad-supported online ecosystem also provides significant benefits to society more broadly. It connects communities and provides increased access to job opportunities, education, and financial information in addition to entertainment content. 81% of regional Australians responded that ad-supported digital content and services enabled them to more easily able to stay in contact with friends and family[2]. Importantly, ad supported online content and services

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

[2] Ibid.

are most important to lower income consumers. The perceived value of free ad-supported digital services and content is twice as high (relative to income) for lower income households.[3]

The changes to our privacy regime should not stifle further innovation or advancement in the industry and not unduly hamper the digital ecosystem, which has been developing ways to thrive in a privacy conscious manner within evolving regulatory frameworks. The creation of new Australian privacy laws that are out of step with and go further than other key markets will create undue restrictions for the Australian market.

The MFA is concerned that some of the Report's proposals may:

- mean Australian privacy laws are inconsistent with, and more onerous than, privacy laws in other jurisdictions; restrict digital advertising, and the availability of free services online;
- create barriers to entry particularly for smaller businesses and place larger and more established corporations at a competitive advantage;
- create significant practical consequences for business, advertisers, and the media industry; and
- have unintended detrimental impacts for consumers and the community.

More generally the overall impact of some of these proposals may introduce the following challenges:

- Compliance costs: Businesses may face significant costs to comply with new privacy regulations, potentially hindering growth and innovation particularly with small business;
- Regulatory complexity: This can result in confusion for businesses and consumers and can discourage investment and involvement in the Australian market;
- Potential for overregulation: Overregulation may stifle innovation and hinder the development of new technologies and services; and
- Competitive disadvantage: Australian businesses will be at a disadvantage to those in countries with less strict privacy laws which can make it harder to grow and compete for global customers.

Key Issues with the Report proposals

In this submission we outline the MFA's perspective on key issues with the Report proposals and provide information to support our views. The key concerns are in the following areas:

1. Targeting: the definition of 'targeting' is excessively broad and captures information even if an individual is not identifiable or reasonably identifiable. This is not workable, when you consider practical media industry considerations such as the requirement to exclude certain audiences from certain ads, and the undue impacts on audience segmentation practices very commonly relied on by advertisers. Further the right to opt out of targeted advertising is unqualified, which raises significant practical concerns. These requirements go further than other key jurisdictions. Unintended consequences include businesses being unable to effectively comply with their legal and social obligations in ensuring that children or vulnerable people are not targeted;

[3] Ibid.

2. Consent, and Privacy by Default Settings – the requirement for consent to be unambiguous, may in practice remove the ability to rely on inferred opt out consent which is regularly adopted across the industry. The privacy by default framework can unduly restrict the availability of commonly expected and socially beneficial services and features, may have undue detrimental impacts on business and place undue burden on consumers;

3. Fair and reasonable requirement – this goes further than other key jurisdictions and introduces significant ambiguity and uncertainty for businesses and the community;

4. Trading – the definition is extremely broad and goes well beyond what is commonly understood as trading of data which can have significant practical consequences.

Further, the MFA supports the introduction of a 'legitimate interests' framework as a lawful basis for use of data, which can assist with providing certainty and addressing some of the issues above.

Key Issue 1 – Targeting (Proposals 20.1 – 20.9)

1.1 The issues with the Targeting proposals are:

- The definition of 'targeting' is excessively broad. It captures information which relates to an individual, regardless of whether they are identified or reasonably identifiable. This means it would also encompass broad and basic segmentation.

- This takes the concept of targeting well beyond the commonly understood meaning of the term or the scope of activities that should be regulated by privacy laws. This is not workable in our view.

- The proposed definition is inconsistent with other key jurisdictions – importantly it goes further than GDPR or the UK.

- Further, the right to opt out of receiving targeted advertising is unqualified, which is unworkable.

1.2 Excessively broad 'targeting' definition

These proposed changes to the definition can have significant adverse and unintended consequences which are set out below.

This definition now includes de-identified and unidentified information. In practice, this takes the definition well beyond the understood meaning of targeting and extends this further into segmentation. This definition of targeting would encompass and include any and all segmentation, regardless of whether any person is identified or reasonably identifiable, and no matter how broad the category or the number of people included in the segment.

1.3 Segmentation considerations

By way of background, in the advertising and media industry:

- Segmentation, is the process of finding big clusters of people who are part of an audience, and this is done on very large, broad and basic parameters including behaviour or geographical area);
- Segmentation is generally treated as a different concept to targeting. Targeting can be more identifiable, granular, and specific, for example, an advertiser wants to find new customers so will exclude current identifiable customers from a campaign.

The concern is that the proposed definition of targeting bundles these two practices together. There are very different considerations here, as to whether or not consent and opt out requirements are appropriate or relevant for:

- an identifiable individual receiving a targeted advertisement which has been targeted to them personally and directly, based on their personal information, as opposed to:
- audiences receiving advertisements where there may have been segmentation or targeting on a broad, general, aggregated and/or non-identifiable or de-identified basis.

Notably in the GDPR and the UK there is no opt out right for targeting generally, rather the right to object applies to carefully defined direct marketing using personal data, as we consider below.

The inclusion of segmentation into the concept of targeting, regardless of whether a person is identifiable, will mean that practices are regulated as 'targeting' even where essential for operational or legal purposes. This would have significant impact on the ability of advertisers to segment online audiences in ways that are important, and not related to any individual.

Segmentation is a critical part of digital advertising. The vast majority of digital media campaigns are currently delivered using some form of targeting or segmentation, including at the very least using geographical information to be able to identify and deliver to the correct audiences, such as in Australia or NSW only. This is fundamental to ensure that advertisers are allocating their advertising investment effectively and to the right audience, but also to meet their regulatory and social obligations.

Some of the practical considerations and unintended consequences can be illustrated as follows:

Currently businesses regularly use segmentation of online audiences to reach the appropriate audience, but for a range of other reasons including critically, to meet their regulatory compliance, social and community obligations.

(a) Basic geographical segmentation

Currently businesses can use geo-location data to segment large chunks of the country's population and only address their advertising to consumers that can access that service. Charities, businesses and government bodies can also use this data for precision targeting to direct important messaging to residents of a particular area.

For instance:

- An offer or service or message that is only available to residents of a particular state, such as a solar panel rebate offer, or a 'go in the draw for a chance to win' competition, a telecommunications provider that only offers certain services to a certain group of postcodes, or a roadside assistance company that can only service residents in NSW.
- Local or small businesses that only service a certain area.
- Important public health and community announcements, such as bushfire or flood alerts, or vaccination adoption or lockdown or other public health messages,
- Political or election related advertising,
- Charitable initiatives,
- Government public messaging on issues such as road safety or water use which can be specific to certain areas or affected communities.

It has been well established through the course of the COVID-19 pandemic that the ability to direct messaging to residents of certain States and Territories in Australia is critical for community and public health purposes.

The ability to segment in different States is critical for advertising in Australia even more so than other markets as Australia is a vast country, it is organised as a federation meaning many businesses, charities and Government bodies only operate in certain states.

Advertising an offer or competition or service across Australia could lead to a business being inadvertently liable for misleading consumers as to the availability of a service that is not available to audiences in those areas. If an advertiser cannot identify someone as a NSW resident as opposed to a Victorian resident, then individuals can potentially receive ads for offers or services which are not open to residents in their State and which may not comply with the laws of their State and be contrary to the Australian Consumer Laws.

Advertisers may find themselves targeting outside their service zones. Advertisers who are only able to service a certain area such as NSW, have a responsibility (as well as for cost and practicality reasons) to ensure that only people in NSW receive advertising for those offers or services. Online advertising does not have the analog framework (namely, transmission zones or time slots for TV and radio, or geographical placement controls for out-of-home) that can assist in other media such as out-of-home or TV. Therefore, online advertising heavily relies on segmentation to be able to achieve these fundamental placement requirements.

This could also mean that it becomes infeasible to communicate locally relevant messages such as those for bush fires or for localised postcode only offers.

There may be a consequent rise in consumer frustration in receiving advertising and offers that fall completely outside of where they can access them.
Many businesses (and particularly small to medium businesses) need to only target advertising to its delivery area or service area. Removing postcode or similarly based targeting will reduce effectiveness or advertising options to those who most need local advertising options to generate commerce. Postcodes for example, are not personally identifiable but may in any event be included in the scope of "targeting".

(b) Demographic and behavioural data

Advertisers often use other basic demographic and behavioral data to infer information about a user, and then use this information to segment audiences so that they are able to include and in many cases excluded audiences. .

A practical example of inferred data is where a person has no Google account, but they go on Youtube and watch Peppa Pig videos. Google may infer from this behavior that this person is a young child or parent. So, when a bid request comes in for an alcohol brand, Google will refer to that data in placing ads for that alcohol brand. The advertiser (or its agency) is able to set bid parameters which will include for example, no advertising to children. These parameters and settings need to match what data the media publisher (eg Google) has for the audience. So, the publisher (eg Google) can infer who that person is, by their behaviour even if they do not have all of that precise data (such as their actual age). They make assumptions and inferences based on their behaviour.

This is where the use of clean rooms and anonymised data are already being used to address privacy concerns. For instance, an advertiser may have data including identifiable information, which is sent to a third party platform to create a custom audience but it is anonymised through the process. When data is used to exclude people under 18, or for geotargeting, the advertiser may not have access to any identifiable data in respect of that audience.

There is a risk that requiring consent or imposing a blanket right to opt out of all targeting including segmentation, means that the use of this information will be significantly restricted in practical terms in ways that are unintended.

Lack of access to this inferred and unidentifiable data for basic segmentation purposes, would have damaging consequences.

Advertisers will not be able to use this data to comply with regulatory requirements that equally apply to them. For instance:

- Alcohol and gambling brands who currently rely on this data to exclude children from their advertising;
- Occasional food and beverage brands (such as chocolates, biscuits, certain fast foods, soft drinks) who are subject to legal obligations under AANA advertising codes to not target children, and need to use this data to ensure that children are not targeted in their online audiences; and
- Advertisers who only have offers applicable to certain States who use this data to ensure the offers are shown to residents of those States, as above.

There can also be social and community focussed benefits associated with ensuring that messaging is appropriate to the relevant audience and this may be done on a broad, or a more specific basis. For instance:

- Ensuring that those in vulnerable groups are excluded from advertising for certain products, such as being able to not advertise credit cards to those who may be experiencing financial hardship;
- Note the Origin Energy case, in 2021 where it was found to be in breach of the national energy retail laws for breaching obligations to protect vulnerable customers unable to pay their bills due to hardship, demonstrates the importance of being able to ensure that advertisers need to be able to ensure it can offer individualised and tailored offers to consumers, and exclude vulnerable consumers from certain messaging;
- Helping charities to maximise investment to potential donors;
- Certain age groups seeing advertising for services and initiatives that are of benefit to them, for instance senior's health services or pension changes or pensioner only rebate offers; and
- Precision targeting to certain demographics or audiences can also be important to drive uptake on important public health issues such as vaccine adoption.

1.4 Unqualified opt-out right to targeting (Proposal 20.3)

An unqualified opt-out for the use of information (including inferred, or non-identifiable information) for targeting purposes can have economic and consumer impacts that are not justified in protecting privacy. This may have the unintended consequence of meaning that platforms and advertisers will not be able to effectively control or screen who sees their ads. This will mean in practice they advertisers are either forced to:

- Use a much smaller pool of those who have opted-in, thus excluding many from important and beneficial messages, or
- Move to a default of advertising to everyone in Australia, thus causing not only a negative experience for consumers but also regulatory breaches for advertisers who need to ensure they are only showing their messages to appropriate audiences, but are required to do so by other applicable laws.

We note that the GDPR (Article 21, for EU and the UK) provides individuals a right to object to processing of their personal data for direct marketing, including profiling for the purpose of direct marketing. However, this is applicable in respect of a person being targeted for direct marketing as an individual, and not more broadly to all targeting or segmentation on a non-identifiable basis.

There are separate requirements for tracking technologies and significantly, some of these are currently being wound back in the UK when it comes to cookies.

Importantly, the GDPR and UK have the 'legitimate interests' test as a recognised basis of use.

Further on this, when the GDPR opt out right for direct marketing is referred to as being absolute, (or 'unqualified'), this means that carveouts otherwise available (such as elsewhere in Article 21 for processing data based on 'legitimate grounds') do not apply. Without such carveouts in our laws, and especially given the issues above with overly broad targeting rules, the wording of this 'unqualified opt out' is overly onerous, is not workable.

We are concerned about an unqualified targeting opt out right which is broader for the Australian market than other jurisdictions. This would be a significant deterrent to investment in Australia and raise undue complexity and practical difficulty in this area for businesses and consumers.

1.5 Further comments on the targeting proposals

Advertisers, large brands as well as small businesses rely on the effectiveness of digital marketing and advertising to find and attract the right customers. Targeting has been shown to improve the return on investment with ad spend, reduce the cost of achieving sales, and improve the quality of leads, so this can be of great advantage to business, particularly those with smaller budgets. This effectiveness is largely due to the use of inferred and unidentified data as a baseline. The disruption of this base layer would inevitably have repercussions on the effectiveness of digital advertising, and on the advertiser's ability to find consumers. Especially for small businesses where the cost to entry of alternatives are just too high. Undue restrictions will not be conducive to business growth and investment in Australia.

As can be demonstrated by the above, there are many advantages to consumers, the community and the business economy more broadly to targeting and restricting the ability to utilise targeting and segmentation measures can have detrimental impacts. Exclusion targeting is currently a key technical mechanism available to implement harm minimisation.

The targeting practices that are of concern and that have been the focus of the debate around targeting, are targeting based on personal information. The opt out of targeting as far as it applies to personal information may be acceptable, but close consideration should be given to the inclusion of non-identifiable information, and regard given to allowing legitimate uses to continue.

The proposals on targeting should be carefully considered with respect to impacts on the ad-supported services ecosystem, and to ensure that they do not unduly restrict service customisation and personalisation, such as product recommendations, that are largely beneficial for consumers. Also, clarification is needed regarding how an individual's right to opt-out would work in relation to targeted advertising that relies on de-identified or unidentified information. It is not clear whether the opt out right covers non identifiable data but there are significant problems with this.

Additionally, further clarity is required about how the redefined term 'personal information' will interact with the proposals on targeted advertising.

1.6 Practical implementation of an opt out to targeted advertising

It is not clear whether the burden of opt out sits with advertiser or the platform. In the case of online advertising which can involve multiple actors in the execution of targeted advertising and direct marketing, there are significant concerns and complexities as to how an unqualified opt out would be practically facilitated. To take an example scenario, when a company collects consumers' personal information and obtains consent to use this personal information, the data is used by both the advertiser and by the online platform to match the right user. The burden of opt-out could sit with either the advertiser and/or with the online platform.

From a practical perspective, it would be much easier for consumers to opt-out where they see the ads rather than go back to a brand's property to manage their consent.

It may be appropriate for the opt out to apply to the relevant controller of the data, to whom the individual notifies of the opt out.

However, the current proposal is unclear as shown by the following practical examples.

- A user has provided consent for marketing purposes to a department store such as Myer. As they browse the web, the consumer sees ads for Myer on Facebook, on YouTube and on The Sydney Morning Herald, however, keeps seeing the ads more regularly on Instagram and decides to opt-out.
- They opt-out straight from Instagram when they are in the platform. It could be a reasonable expectation for the consumer to not see any advertising from Myer again, or it could be a reasonable expectation to not see Myer again on Instagram.
- Currently the proposal isn't clear on the impact "opt-out" should have and whether it is attached to an advertiser, or to processing by a platform. The practical implications in each case are very different.

- A user who has a Commonwealth Bank credit card with Qantas points wants to opt-out of their information being used for marketing purposes. The information may sit with Commonwealth Bank and the MFI, Visa as the card provider and Qantas as the loyalty program. At this stage it is unclear if any of the participants are required to offer individual opt-outs or if there is an expectation that an opt-out from one should be understood as an opt-out from all.

Therefore, it is our view that the unqualified right to opt-out should be considered closely.

There are technical considerations of an opt-out mechanism for online advertising that should be considered, as there are three key scenarios for non-traditional direct marketing and online ad targeting:

- In-platform advertising such as social channels (Meta's Facebook and Instagram, TikTok, Snap etc…);
- Owned and operated properties such as news.com.au; and
- Ads delivered programmatically through a complex programmatic supply chain in which data processing sits with various actors along the way.

In this last case it is unclear how an opt-out would work and how the consent management could work across the entire open web.

Facebook has for instance a 'why am I seeing this ad?' facility which users can click, with a pop up which explains the basis behind the ad. This may be feasible within Facebook's 'walled garden' but there are practical questions with how this sort of facility could be implemented more broadly. It is clearer to envisage how to implement an opt-out where there is a single relationship between a customer and a brand, such as with Myer and a customer opting out of Myer marketing materials. However, it is not so clear in an online context, noting the multitude of interactions a person may have and the different relationships in the advertising ecosystem. There would need to be significant investment, time, work and infrastructure involved in a proposal that was intended to work across different participants and an unqualified right in this context would raise serious practical difficulties.

Key Issue 2 Consent and Privacy by Default Settings (Proposal 11)

2.1 Consent requirements (Proposal 11.1 Valid consent)

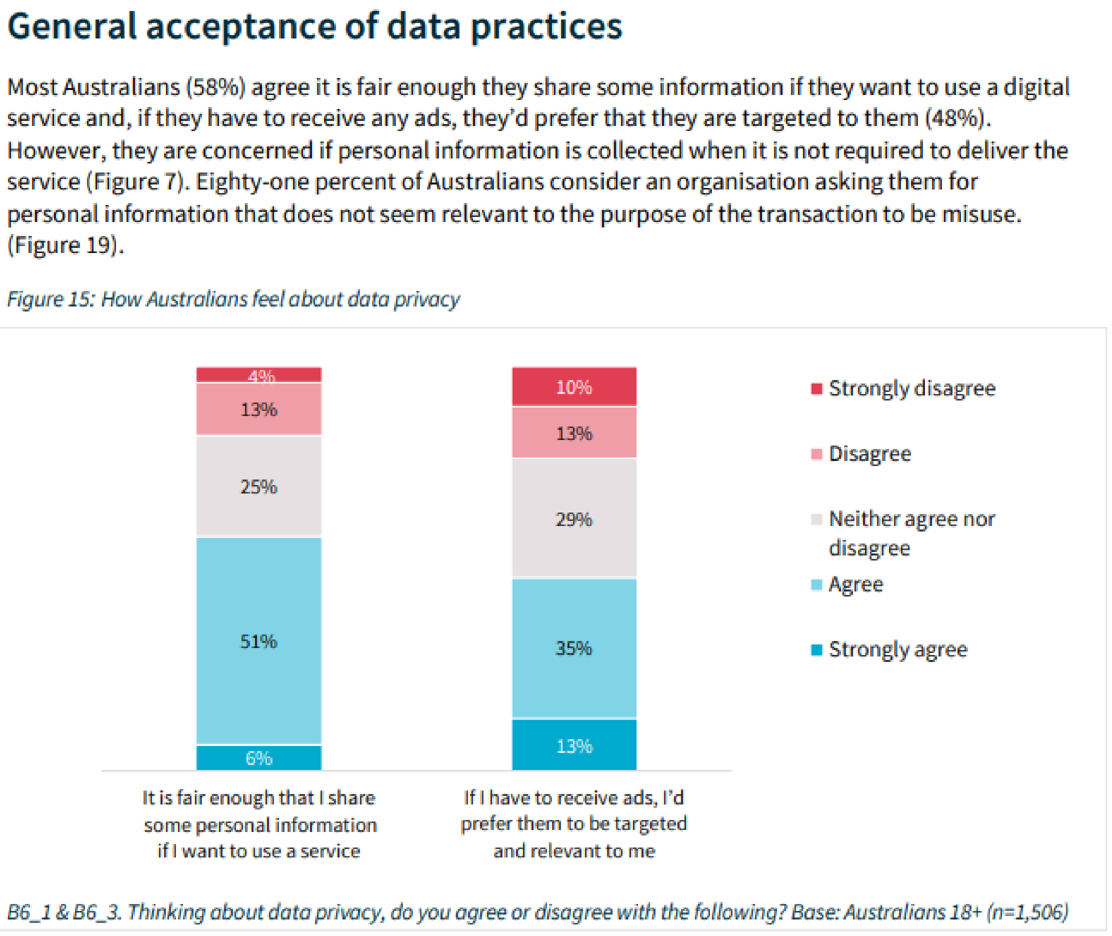
The requirement for consent to be unambiguous explicitly references OAIC guidance that inferring consent will only be appropriate in limited circumstances as the data subject's intention in failing to opt out may be ambiguous. The practical effect of this unambiguous requirement would be to remove opt-out inferred consent as an option which is frequently utilised within the industry.

2.2 Privacy by Default (Proposal 11.4 Online privacy settings should reflect the privacy by default framework)

The privacy by default proposal in our view goes beyond community expectations and may have the unintended consequence of depriving consumers of benefits they expect, but also depriving advertising platforms of the relevant data (eg that someone may be a child) which can enable appropriate exclusion from certain advertising, and be materially detrimental to many businesses that are fundamental to the economy and the media environment.

(a) Community expectations

We note that the Australian Community Attitudes to Privacy Survey 2020 found the following:



General acceptance of data practices

Most Australians (58%) agree it is fair enough they share some information if they want to use a digital service and, if they have to receive any ads, they'd prefer that they are targeted to them (48%). However, they are concerned if personal information is collected when it is not required to deliver the service (Figure 7). Eighty-one percent of Australians consider an organisation asking them for personal information that does not seem relevant to the purpose of the transaction to be misuse. (Figure 19).

Figure 15: How Australians feel about data privacy

4%
13%
25%
51%
6%
10%
13%
29%
35%
13%
🟥 Strongly disagree
🟥 Disagree
⬜ Neither agree nor disagree
🟦 Agree
🟦 Strongly agree
It is fair enough that I share some personal information if I want to use a service
If I have to receive ads, I'd prefer them to be targeted and relevant to me

B6_1 & B6_3. Thinking about data privacy, do you agree or disagree with the following? Base: Australians 18+ (n=1,506)

The above shows a high level of consumer acceptance and expectation by Australians when it comes to the sharing of information when using a digital service and receipt of targeted advertising.

BCG Research* has shown that 74% of consumers prefer ad personalization over non-personalized. Part of an agency's role is to create the best possible experience for the user to help support an advertiser's communication. Ad personalization relies on behavioral based targeting, that could be restricted by default under the current proposal. This would also have a dramatic impact on the revenue of smaller based publishers such as local news publishers who offer behavioral based advertising to fund their operations.[4]

(b) Material detriment to business

We note that previous submissions noted in the Report, have considered that pro-privacy defaults would compromise the ability of certain businesses (such as media publishers) to generate revenue and may 'materially affect' their business models. For instance, it was noted by one publisher that very few customers would opt-in to targeted advertising given that 'consumers rarely change default settings provided to them'[5]. It was noted that the ability of media publishers to use 'data, ratings and aggregate demographic information' to inform decisions about programming on its broadcast platform to better cater to audiences would be

[4] Source: BCG/Google, U.S. and Canada, Consumers Want Privacy. Marketers Can Deliver, Jan. 2022

[5] SBS Submission to the Discussion Paper, 21-22, as noted in the Report, 134.

negatively impacted by pro-privacy defaults[6]. In particular it was noted that free-to-air television is an advertising funded business model and that it is '[i]mportant for the Australian media to require viewers to receive some advertising' as a condition of receiving free online streaming services. The advertising-funded model for the Australian media is well-established, a diversity of media voices is essential to the public good and that the 'the burden on taxpayers of funding multiple Australian media services would be great.'[7]

There will also be a considerable detrimental impact on data collection and measurement of effectiveness of advertising, and this will also restrain the ability of advertisers in being able to send appropriate content to people.

(c) Consent fatigue and related detrimental impacts

We also support past submissions which noted[8] that pro-privacy defaults could result in consent fatigue if entities were required to seek individuals' consent through a change of privacy settings for activities that are essential to the effective functioning of a service.

Consent is often regarded as a desirable, easy-to-use basis for processing personal data that gives choice to individuals. In practice, however, consent can be cumbersome, overwhelming, and ultimately meaningless for individuals who face a barrage of requests without the time or capacity to review them properly. Consent fatigue will only increase if more and more digital interactions require consent as data is collected, used, and shared in the digital economy. This can undermine and devalue privacy protection by discouraging people from reading privacy notices and can even lead to users over-sharing without realising.

(d) Detrimental impacts including depriving consumers of content and services

If companies whose business models are based on personalisation are required to provide a service to those who opt out of any form of personalisation, that company's business model is undermined. Examples of businesses that rely on personalisation include Netflix, Amazon, Apple, Google, Bunnings, Woolworths, loyalty programs and banks, who need to be able to personalise important information to their customers, but many other smaller businesses like fashion labels, hospitality, restaurants and local businesses. If customers are able to opt out of personalisation, these inherently personalised services will not be able to be effectively monetised and these business models may consequently become unviable. The impact on smaller companies, will be greater as they do need to be able to connect and offer the right messages and services at the right time. Ultimately, we are concerned that this will damage consumers due to less freely available content and services.

Another is facial recognition technology in a security context. This new standard may have an adverse impact of those enhanced consent requirements on data collection and processing activities where consent was previously inferred from the behavior of the consumer (or employee), such as entering premises subject to a prominent notice that facial recognition and biometric scanning are being used for security purposes.

Pro-privacy defaults may have unintended consequences in certain businesses such as for instance video games, travel, shopping, news and other online experiences. This could include frustration for users, by requiring them to manually change their settings to access expected features such as selecting a service based on location, enjoying personalised features, and

[6] Ibid.

[7] Free TV Submission to the Discussion Paper, 31, as noted in the Report, 134.

[8] Telstra Submission to the Discussion Paper, as noted in the report, 134.

sharing content. This would in our view be the case with many services across the economy. Consumer expectations are that a certain level of personalisation and use of data has come to be accepted, understood, and expected. As a result, reverting to a high level of privacy by default would not be in line with consumer expectations and may result in consumers being deprived of services, features, and benefits in their online user experience that they have become accustomed to.

A privacy by default setting may also unduly restrict the ability of advertisers to prevent unsuitable content going to certain users. This can have wide sweeping impacts and lead to sub-optimal and ultimately also potentially less safe user experiences.

(e) Inconsistent with other key jurisdictions

We note that this proposal appears to run counter to the UK where they are winding back laws in this area and recognising certain uses of data as being 'necessary'. The UK government has proposed reforms that would remove the consent requirement for analytics cookies (treating those as 'strictly necessary' cookies) and remove the requirement for prior consent for all types of cookies.

Data analytics software is used to gain a better understanding of how websites are used, which can create a better user experience for consumers. Data collection for the purposes of data analysis may be subject to consent requirements under this Privacy by Default proposal. This can lead to sub-optimal customer experiences online but crucially, can leave Australia out of step with laws in other markets which recognise these and other practices over time as 'necessary' or legitimate data uses.

2.3 MFA supported alternatives

Given the problems shown above, the MFA encourages the continued use of opt-out consent (or implied consent) in appropriate settings. The MFA would support a framework which allowed individuals clear ways to set privacy controls as appropriate to them.

The MFA also supports moving away from viewing the traditional consent model as the only way to protect users, and instead establish a model, which allows for other legitimate baseline uses. This puts the burden on businesses, not individuals, to ensure they are within legitimate boundaries and prevent harm, and we believe will help deliver stronger protections for individuals.

2.4 Legitimate interests

The MFA would welcome the exploration of a legitimate interest framework as part of the privacy reforms, as a legal basis for processing data in Australia and an alternative to obtaining consent. This which would help to address this issue and provide a future-proof basis for lawful ways of processing data. The MFA considers that this is consistent with the laws of other key markets which will enable us to draw from the body of case law, regulatory guidance and knowledge being developed in those markets. The 'legitimate interests' test can provide a means of recognising and allowing legitimate data use practices which can be managed appropriately and safely according to the context, as those methods arise over time. This would allow specific types of data to be used to identify and prevent fraud, ensure network and information security and enable entities to use data in ways that are lawful, proportionate and fair to the user. The MFA believes this test is a sensible way to allow entities to use data in ways consistent with customer expectations where explicit consent may not have been obtained or may not be feasible.

Relying too heavily on a requirement for consent, or a blanket opt out right, can stifle or restrict practices that are important for a thriving media landscape and local economy. There are benefits for consumers that may be inadvertently overridden by some of these consent based rules.

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

Key Issue 3 – Fair and reasonable requirement (Proposal 12.1)

The MFA is concerned with the proposal to amend the Act to include an additional requirement, that the collection, use or disclosure of personal information must be "fair and reasonable in the circumstances". We note that this wording is also used in Proposal 20.8 in introducing a specific requirement that "Targeting individuals should be fair and reasonable in the circumstances."

The concern here is that this would go further than the requirements in any other jurisdiction, as shown by the below (Figure 12.1 copied from the Report)[9]:

Jurisdiction	**Law**	**Provision**
Europe and UK	*GDPR and UK GDPR*	**Article 5(1)** – 'Personal data shall be processed lawfully, *fairly* and in a transparent manner in relation to the data subject.'
Canada	*Personal Information Protection and Electronic Documents Act 2000* (PIPEDA)	**Section 5(3)** – 'An organization may collect, use or disclose personal information only for purposes that a *reasonable person would consider are appropriate* in the circumstances.'
Singapore	*Personal Data Protection Act 2012* (PDPA)	**Section 18** – 'An organisation may collect, use or disclose personal data about an individual only for purposes that *a reasonable person would consider appropriate* in the circumstances'

Figure 12.1: Equivalent baseline protections in selected overseas data protection legislation.

The MFA is concerned that each and every collection and use and disclosure will need to meet the ambiguous requirements of being both fair and reasonable. We see the benefits in business certainty in being able to understand and abide by the scope of their legal obligations. In the UK and the EU, a body of regulatory guidance and case law is being developed as to the meaning of the 'fairness' standard in a privacy content, and another body of regulatory guidance and case law is separately being developed in Canada and Singapore as to the meaning of a 'reasonable person' standard in a privacy context. If we are to import both of these requirements into our laws, this brings significant uncertainty for business. Further this leaves Australia with a more restrictive and onerous compliance environment than any of

[9] Report, 141

these other jurisdictions. This can in turn discourage investment and engagement in Australia and raise the barriers to entry particularly for smaller players. While there is use of the term 'unfair' in relation to unfair contract terms requirements in Australian consumer law, the term 'fair' does not have precedent in Australian law and is not sufficiently defined in the proposal. Further consideration and guidance is required in this area.

The MFA welcomes and supports the introduction of a 'legitimate interests' test as set out above, which can assist with providing certainty. We note that a Bill has been introduced in the UK (the Data Protection and Digital Information Bill, laid before Parliament in July 2022) to clarify a recognised list of activities considered to be legitimate interests, including direct marketing, intra-group transmission of personal information and ensuring the security of network and information systems. This Bill is said to form a crucial part of the UK's National Data Strategy which aims to show opportunities for 'unlocking the value of data' and 'securing a pro growth and trusted data regime', while retaining the UK's adequacy status under GDPR. We see benefits in our laws being aligned with these developments so that our businesses are not at a competitive disadvantage in these impacted areas.

Key Issue 4 – Trading (Proposal 20.1)

4.1 Key concern

The MFA has concerns with the proposed definition in Proposal 20.1 for Trading –"Capture the disclosure of personal information for a benefit, service or advantage". This is in light of the related Proposal 20.4 that consent must be obtained from an individual to trade their personal information.

The definition of Trading is extremely broad, not limited to what is commonly understood as trading of data but also appears to include any form of sharing of data or potentially even verification of data points with partner organisations or group members.

4.2 Some practical examples

To illustrate the verification of data points referenced above, Google may hold a data set for an audience. An advertiser or a media agency may also wish to use a third party such as comScore or Nielsen to verify that data to check that they are for instance targeting a male over 18. There is an exchange of data in that instance, and this appears to be caught by the definition of trading.

In the concept of trading as envisaged in the Report, there was a focus on data brokerage services whose business model is based on trading in information relating to individuals, who then sell that information to third parties including marketers. The proposed definition however goes well beyond these sorts of activities.

Some use cases that can illustrate this include the following:

- IDs shared within clean rooms for ID resolution – Data enrichment purposes;
- Unified data solutions for ad targeting and measurement;
- Automated data trading to third parties for core digital and ecommerce functions – onsite personalisation, offsite retargeting etc;
- Data traded between government departments;

- Media agencies may in practice obtain aggregated data from various third party data providers such as Oztam, Nielsen and so on, and also from the client. The data may be provided to the publisher but via an anonymised process which can then be used by the publisher to target a particular audience.

4.3 Disadvantages to smaller businesses

We note that more businesses are moving towards greater reliance on first party data (namely, data that has been collected directly by that party from its own audience, customers or followers) and away from second and third party data sets (namely, data collected and provided by third parties, such as via third party cookies). Restrictions such as those on trading of data without consent will accelerate this reliance on first party data in our view. This can mean a greater advantage to those larger and more established businesses who have access to large and valuable first party data sets of their own (such as notably the digital platforms). Larger businesses and agencies are also able to rely on tools or processes that reduce the reliance on identifiable data. However smaller businesses may not have these resources available. Unduly onerous restrictions can place smaller businesses at a competitive disadvantage in restricting access to data in the intervening time.

4.4 Unforeseen consequences for children

The Report also provides in Proposal 20.7 for a blanket prohibition on trading in the personal information of children.

There are significant practical problems with this, as advertisers must be able to meet legal requirements to avoid targeting of certain advertising to children, and the sharing of data for this purpose may be required to ensure these requirements can be properly met and verified.

4.5 More onerous regulation than other key jurisdictions

This trading definition and related restrictions would be more onerous than the regulatory requirements in other key markets.

Trading under GDPR and in the UK is dealt with by more targeted requirements on tracking technologies, but there is no specific requirement to obtain consent in these circumstances. The GDPR and the UK do not include specific obligations for trading in personal data. Rather trading is dealt with as a form of processing, and organisations can do so as long as they can rely on one of the lawful bases for doing so (and these lawful bases include consent, or legitimate interests).

In addition, sharing of data is also already captured by a range of new requirements proposed in the Australian Report:

- the proposed new fair & reasonable requirement
- the new requirement on collection of data from third parties (the proposed new obligation to ensure the original collection as lawful).
- Geolocation proposal.

4.6 Comments on related matters to this proposal

The scope of the trading proposal has been limited to personal information. However, the proposed changes to the definition of personal information, particularly around whether a person is reasonably identifiable, suggest that if you share data with a third party organisation that has the ability to re-identify, then this will involve a disclosure of personal information. The MFA considers that it should be clarified in related guidance to the definition of 'reasonably identifiable' that it is not a disclosure of personal information if the organisation who receives de-identified information has operational mechanisms in place to prevent re-identification, even if they have the technical means to enable re-identification.

It should also be clarified, when 'consent' is required for 'trading' under Proposal 20.4, whether this is opt-in or opt-out, and to consider appropriate exceptions.

In respect of Proposal 20.9 (requiring entities to provide information about targeting including algorithms and profiling) it is important that guardrails are in place to protect confidential information as these may be sensitive to the business in question.

Further Consultation

The MFA would welcome the opportunity to discuss in more detail the issues raised in this submission. The MFA would also welcome the potential for involvement in further consultation in relation to Australian privacy reforms.

Sophie Madden
CEO, MFA
Email: sophie@mediafederation.org.au
Mobile: 0408 613 904