ADMA Association for data-driven marketing & advertising

Submission in response to the Privacy Act Review Report 2022

Australian Government, Attorney- General's Department

8 April 2023

The Association for Data-driven Marketing and Advertising
Level 27
100 Barangaroo Road
Sydney NSW 2000
ABN: 53 156 305 487

1. Introduction

The Association for Data-driven Marketing and Advertising (**ADMA**) welcomes this opportunity to make a submission to the Attorney-General's Department (**AGD**) in response to the Privacy Act Review Report 2022 (**Report**). This is an important consultation and reform proposal, as implementation of the canvassed changes would have substantial and long-lasting impact upon Australian society. ADMA welcomes the AGD's ambitious, but deliberative and consultative, approach in progressing reform.

Throughout its engagement with the Privacy Act Review (**Review**) consultations, ADMA has stated support for reform. ADMA endorses the approach outlined in most Proposals in this Report. Some Proposals are overly broad, not consistent with emerging best practice in comparable jurisdictions, globally and potentially adverse to consumer welfare and the Australian economy. These Proposals, as identified in section 4 below, warrant further consideration.

ADMA's submission outlines positions that our members from across the data-driven marketing industry have expressed to us.

This submission includes:

- General comments that are important as background to the position we have taken;
- Use case scenarios to help illustrate the potential impact of applying the Report's Proposals;
- A summary of ADMA's position for or against key Proposals;
- Detailed explanations of ADMAs position in relation to the Proposals; and
- Other recommendations

The following Executive Summary points frame ADMAs response to the Report.

1. Executive Summary

1. ADMA continues to support moves to enhance privacy safeguards for Australians.

2. ADMA supports many of the Proposals put forward in the Report, some as recommended and others with minor amendments.

3. While ADMA supports the intention behind the approach adopted in the Report, some of the Proposals as drafted will effect little protection from bad actors and instead be burdensome on good actors, confusing for affected individuals, and in some cases effect substantial societal detriment for limited benefits.

4. ***Direct Marketing, Targeting and Trading:*** One focus of ADMA's submission relates to Direct Marketing, Targeting and Trading. The relevant Proposals in this area would increase uncertainty and add unnecessary complexity to the existing compliance framework in the digital marketing sector.

5. ***Definitions too broad:*** Proposed definitions of Direct Marketing, Targeting and Trading are too broad, causing ambiguity. Overly broad coverage (beyond reasonable scope, as discussed in this Submission) will adversely affect quality and range of services available to

citizens and create unnecessary confusion and complexity for APP entities implementing changes to systems and processes and data handling practices as required to give effect to the proposed reforms.

6. *Consent/ opt out fails to protect from most important privacy harms:* Consent based/opt-out frameworks don't solve for inappropriate data collection and data abuse by bad actors. These frameworks also promote unrealistic expectations of many consumers that they will never see an audience segmented ad. Explanations as to use of broad audience segments are often confused with much more granular personalisation through profiling. Attempts to explain uses of privacy enhancing technologies (**PETs**) for effective anonymisation may lead to consumer confusion and have the counter-productive effect of creating disincentives for adoption of PETS and effective anonymisation. Opaque and harmful targeting should be addressed, not broad audience segmentation.

7. *Application of Proposals highlight impracticality:* Applying the Proposals to use case scenarios reveals concerns with the approach adopted and the compliance burden that will be imposed on APP entities, the potential confusion data subjects will face and the failure to protect against the actions of bad actors.

8. *Unintended/ secondary consequences don't seem to have been considered:* The amendments fail to preserve situations where certain types of data collection are necessary to protect users, young people, protect data security, comply with other requirements (i.e., not to market products to consumers where an APP entity ought reasonably anticipate would cause them financial hardship) or consumer expectations (i.e., not to be marketed for a product or service that they already have or that is inappropriate for their needs).

9. *Litigation driven enforcement: The proposed direct right of action may lead to uncertain but potentially costly litigation exposures from plaintiff class action lawsuits, particularly if plaintiff lawyers may litigate as to whether a data handling practice is "fair".* In an increasingly digital society and economy, this may create significant economic and social uncertainty and discourage innovation and investment in the digital economy

10. *Not everything can be regulated through the Privacy Act:* An underlying theme of the Report and Proposals is the need to address perceived consumer harm from "big data" and "big tech". The Proposals should focus upon addressing recognised categories of privacy harms to affected individuals. Other consumer harms, such as harms caused by misleading practices such as use of 'dark patterns', or arising from use of unfair contract terms (including inclusion of unfair provisions in a privacy policy or privacy notice), should be addressed by Australian Consumer Law. Harms to competitive neutrality and the Australian economy should be addressed through competition law.

11. *Regulate for the outcome:* There is a need to clearly categorise the forms of behaviour that should be prohibited or subjected to guardrails or heightened controls, and then legislate to effect that outcome.

12. *Need for further consultation in some areas:* ADMA believes this Review will benefit from more in-depth, solution-specific consultation across industry verticals (federal, state and local) and certain use cases (for example loyalty and financial services), as well as a focus on how to protect sensitive data sets from abuse/misuses (i.e., for protection against hacking and other malicious activity and to ensure national security).

2. General Comments

Good marketers value privacy

Some privacy advocates and civil society organisations view digital marketing as a key area of privacy problems. There is a misconception that digital marketers care only about protecting their ability to do business with minimal practical impediment or regulatory restriction. This is far from the truth. Responsible marketers put their customer at the centre of their focus. Responsible marketers are adopting privacy enhancing technologies (PETs) and safeguards and associated controls for effective anonymisation. Activities of irresponsible marketers and bad actors can and should be addressed without reducing incentives for adoption of responsible marketing practices. ADMA advocates for marketers to protect consumer privacy for the simple reason that, the data-driven marketing and advertising industry's livelihood and reputation depends on it.

> *"Marketers rely on consumer trust more than most divisions within an organisation. As an industry, marketing is driven by protecting consumers from privacy harm. While it can be easy to paint all of marketing with the brush of bad actors (and the mistakes of responsible marketers) - the reality is that the marketing industry spends a lot of time building value and trust in the databases we're now trying to protect with privacy laws. Ensuring safe, responsible, and reasonable use of data is intrinsically aligned to consumers willingness to engage with our brands. A marketers success can be made (or fail) if that consumer trust is broken. ADMA's core position of advocacy in relation to data compliance is "regulation where regulation makes sense – but best practice always".*[1]

ADMA shares the Government's desire to protect consumers from harm. No responsible marketer wants data-driven marketing used in a way that endangers people, contributes towards discrimination, causes harm to children, or sees the most vulnerable in our society made worse off. Use of data in responsible marketing is compatible with a safe, fair, sustainable and prosperous economic future of Australia. Consumer protection and data privacy must operate in tandem in a data-driven society. As we envisage a new regime for "privacy" and "privacy control", we should focus upon data 'abuse', not data 'use'[2].

'Catch-all' proposals confuse APP entities and data subjects without catching out bad actors

In designing a privacy framework that protects individuals from privacy harms, we should also protect an APP entity's ability to provide the benefits that consumers and other citizens have come to expect, such as 'tell us once', don't market products or services that are inappropriate to what you should know are our circumstances, needs and preferences, and provide us with useful information that you reasonably think we ought to know and that aids our decision making. ADMA is concerned that the Proposals relating to Targeting as outlined in the Report could lead to consumer confusion and are more likely to negatively impact the two-way value exchange consumers have with business (APP entities) without actually improving privacy or otherwise creating benefits to consumers.

---

[1] Sarla Fernando – speaking at "A manifesto for a better internet" - Advertising Week APAC, 2022

[2] Joshua Lowcock as part of an Interview with ADMA in 2022 – 'ADMA Regulatory and Working Group Member Profile"

ADMA and our members note the Report fails to recognise that bad actors operate outside the law. The use of broad definitions may be an attempt to cast a wide net that *may* encapsulate activity that has no regard for the law, however this approach risks just creating barriers for businesses to access consumer markets across emerging digital platforms. Small and medium size businesses (SMEs) will be especially impacted. SMEs are at the crossroads of a difficult path to recovery after a pandemic that saw them lean into digital solutions that leverage data to keep their heads above water. They would now face a further deluge of compliance activities and associated regulatory burden. This would adversely affect the ability of SMEs to engage in the digital economy and to compete with more established and global entities, negatively Impacting consumers through increased prices, reduced choice and restriction of access to products and services.

The cumulative effect of Proposals is far reaching

The cumulative effect of the Proposals is particularly problematic, although many of the Proposals taken in isolation do not appear exceptional or unusually burdensome.

For example, the proposed extensions in key definitions have significant knock-on effects in relation to later Proposals which might not be considered particularly burdensome if key definitions continuing to operate as interpreted in the Commissioner's current guidance. There is a substantial risk of misunderstanding as to the likely scope of operation of later Proposals and the envisaged legislative package as a whole, arising from complexity of interrelationships between Proposals.

It may be appropriate to consider a two-stage approach, where key elements of the new legislative framework are first refined and defined, and then as a second stage, new issue or topic specific rules are developed and assessed against those key elements and as applied to specific use case scenarios. This would better enable impact assessment and mitigate risk of unintended overreach. The effect of the envisaged legislative package as a whole might either be constructive, or destructive, of consumer welfare and economic activity. This package will substantially impact the value that consumers derive in their exchange with brands, and the value that brands deliver to consumers, and impact other operation of the digital economy. A two-stage approach would assist in getting this balance right.

A two-stage process would also assist APP entities (including government agencies) to better understand how and at what cost their data structures, data labelling and ontologies, and data handling practices, could be evolved to address new legislated requirements. Many APP entities will need to undertake substantial technical reengineering, and therefore project planning and management, to give effect to some of the Proposals. It is important to define the scope of operation of these Proposals by taking into account their likely impact upon how APP entities (including government agencies) currently enable and control uses of data relating to individuals, and the costs and complexity of transitions to a new legislated framework.

Use case applications are useful to assess whether intent of recommendation is the actual outcome

ADMA has significant concerns regarding the Proposals in section 20 of the Report. The impact of these Proposals on the digital marketing industry (from both an APP entities' perspective and in relation to customer experiences), and subsequently all marketing divisions from all companies, would be very substantial.

For example, the definition of targeting, is recommended to cover tailoring of services, content, information, advertisements or offers provided to or withheld from a consumer. The definition is (possibly) deliberately broad in a way that encompasses both individualised addressable targeting and general broad-based cohort targeting. This creates both a compliance and consumer dilemma while disadvantaging certain members of Australian society.

At ADMA, we appreciate the desire to give consumers the ability to opt-out of the use of their data in a personalised experience e.g. unsubscribing from an email. However, in cohort-based marketing activity, an individual may feel "targeted" simply because the message has a high degree of relevance, not necessarily because their data was used, creating cognitive dissonance for consumers who expect to be able to opt-out from any relevant advertising when an opt-out is not possible

Further, ADMA has concerns that under the prescribed definition, targeting would even encompass key federal, state, and local government related advertising, specifically in services that protect the vulnerable e.g. COVID vaccination availability, smoking cessation advertising, or access to local community services for the elderly.

When it comes to certain types of data, such as location, ADMA emphasises a need to consider the unintended consequences of a definition of 'geolocation tracking data' as personal information (and requiring consent). From a practical standpoint, the absence of consent would inhibit police geotargeting messages that advise people in a local area to keep an eye out for a missing vulnerable person in their community; or local emergency services providing relevant updates in time of crisis.

Further, the absence of considering the abuse of location data means what may be considered sensitive national security locations e.g. Australian Parliament House, ADFA, Lucas Heights, etc. would all be reasonable to collect precise user location data provided consent was obtained. This gets to the heart of what ADMA believes must be considered by regulators - that in most instances it is the potential (mis)use and/or abuse of the data itself that needs to be examined when developing new regulations, not simple broad definitions of categories and types of data.

Need for Regulatory Consistency

A need for careful reflection is heightened by the fact the privacy law review is not the only form of regulatory development taking place in Australia. The Government is currently also in the midst of reviewing the Australian Competition and Consumer laws, cybersecurity and e-safety regimes. Each of these regulatory frameworks are applied to APP entities in different ways and may have a direct bearing on the way personal privacy is maintained, protected, enforced and understood.

In our discussions with various industry sectors, it was highlighted that sector specific regulation may be easy to implement on its own, but when trying to balance with other compliance requirements, they face difficulties. For example, financial services members gave real-life examples of situations where they try to balance Know Your Customer (KYC) requirements and other financial industry regulations from a tax, compliance, data retention, and security perspective. A genuine fear in this Review is that a revised privacy statute will add complex layers of conflict, increasing anxiety around ensuring companies are in full compliance across the various legislation, industry codes, best practice requirements and more.

Digital marketers and compliance personnel are endeavouring to comply with multiple, disparate and rapidly evolving statutes and delegated regulation, including many new industry codes and standards. The burden upon APP entities particularly impacts and disadvantages SMEs. Regulatory complexity, and myriad interactions and possible inconsistencies across regimes, needs to be recognised and mitigated wherever reasonably practicable.

More consultation, now, will better inform a fit for purpose Act.

3. Summary of ADMA's Positions on Proposals

Number	Proposal summary	ADMA Position	Key Note	Page
3.1	Objects of the Act to clarify 'PI'	Support	Implement proposal	
3.2	Amending Objects of Act to recognize public interest in protecting privacy	Support with Amendment	Support, with recommended tweak	15
4.1	Change' about' to 'relates to'	Support	Implement proposal	
4.2	List of examples	Support with Amendment	Support but example should be in guidance, to facilitate evolution	15
4.3	Amend definition of 'collect' to include inferred information	Support	Implement proposal	16
4.4	'Reasonably identifiable' to be supported by a list to which APP entities may have regard	Support with Amendment	Implement proposal but clarify that each 'circumstance' requires a case by case, contextual evaluation	16
4.5	Amend definition of de-identified	Amend	Needs to be clearer: should only relate to information reasonably capable of enabling identification when available in another context	16
4.6	Apply some APPs to de-identified data	Amend	Only information reasonably capable of enabling identification when available in another context, and then only for defined and limited contexts that do not include use in broad audience segments	17
4.6	De-identified in relation to targeting	Concern	Too broad, further consultation is appropriate	18
4.9	Amend sensitive information	Support	Implement proposal	
4.10	Geolocation Tracking Data	Concern	Consider application of the definition of 'geolocation tracking data' to be limited to sensitive locations	19
6.1	Small Business Exemption	Support	Implement proposal	20
6.2	Small Business Exemption	Support	Implement proposal	20
10.1	Clear, up to date, concise and understandable collection notices	Support	Implement proposal NOTE: Position changes if proposals 19 and 20 go ahead	21
10.2	Matters to include in a Notice	Support	Implement proposal	21
11.1	Definition of consent	Support	Implement proposal	
11.2	Consent Request design	Support	Implement proposal	
11.3	Withdrawal of Consent	Support	Implement proposal NOTE: Position changes if proposals 20 and 19 goes ahead	21

Number	Proposal summary	ADMA Position	Key Note	Page
11.4	Accessible Privacy Settings	Support	Implement Proposal	
12.1	Fair and Reasonable Test	Support with Amendment	Support test as to reasonableness, unfair contract terms and misleading business practices should continue to be addressed by Australian Consumer Law, affirmative obligation of "fairness" too subjective and likely to fuel plaintiff class action lawsuits	22
12.2	Fair and Reasonable Test Matters	Support with Amendment	Support if test is as to 'reasonable(ness)', not as to 'fair(ness)'	22
12.3	Fair and Reasonable Test to apply when consent was obtained	Support with Amendment	Support if test is as to 'reasonable(ness)', not as to 'fair(ness)'	22
	PIAs for high-risk activities	Support	Implement proposal	
13.2	Enhanced Risk Assessments for FRT	Support	Implement proposal	
13.3	Practice Specific Guidance for new technologies and emerging privacy risks	Support	Implement proposal	
13.4	Third Party collection requirements	Support	Implement proposal	
15.2	Senior employee responsible for Privacy	Support	Implement proposal	
16.1	Define child in Act	Support	Implement proposal (so long as it aligns with other local legislation)	
16.2	Children's consent	Support	Implement proposal	
16.3	Clear and understandable collection notices/ privacy notices – children	Support	Implement proposal	
16.4	Best interest of child	Support	Implement proposal (with more appropriate overarching test)	
17.1	OAIC guidance on vulnerability	Support	Implement proposal	
17.2	Supported decision making	Support	Implement proposal	
18.3	Erasure	Support	Implement proposal	23
19.1	ADM in privacy policies	Amend	More consultation needed to ensure this isn't a blueprint for bad actors	24
19.3	Right to obtain meaningful information	Amend	Limit public request to include a right to obtain a human review of a decision made by ADM only	24
20.1a	Definition of Direct Marketing	Amend	On its own OK- Needs to be amended to clarify guardrails to not slide into targeting definition	26

Number	Proposal summary	ADMA Position	Key Note	Page
20.1b	Definition of Targeting	Concern	Too broad, further consultation is appropriate	27
20.1c	Definition of Trading	Amend	Too broad, further consultation is appropriate	30
20.2	Direct Marketing opt out	Support with Definition Amended	Implement if 'direct marketing' definition is clarified to not overlap into targeting	26
20.3	Targeting Opt-Out	Concern	Too broad, further consultation is appropriate	28
20.4	Trading	Amend	Too broad, further consultation is appropriate	30
20.5	Direct Marketing to children	Support with definition amended	Support so long as definition of Direct Marketing is changed as mentioned above	32
20.6	Targeting to children	Support with definition amended		32
20.7	Trading in the personal information of children	Support with definition amended	Clarification of 'trading' definition is appropriate	32
20.8	Targeting with overarching test	Support	Support with less subjective overarching test	
20.8 (b)	Targeting based on sensitive information	Support	Implement	
20.9	Information about targeting	Concern	Consultation required	32
22.1	Controllers and Processors	Support	Support with training	
25.1	Enforcement – Civil penalty tiers	Amend	Reduce exposure of SMEs to $50m penalty	33
25.2	Clarify 'serious' interference with privacy	Support	Support (assuming children included in 'vulnerable')	
26.1	A Direct Right of Action	Amend	Support but needs to consider a way of doing this without opening up resource intensive class actions	34
29.1	Privacy law design guide	Support	Implement proposal	
29.2	Regulatory cooperation	Support	Implement proposal	
29.3	Working Group on harmonising privacy laws	Support	Implement proposal	

4. USE CASE SCENARIOS

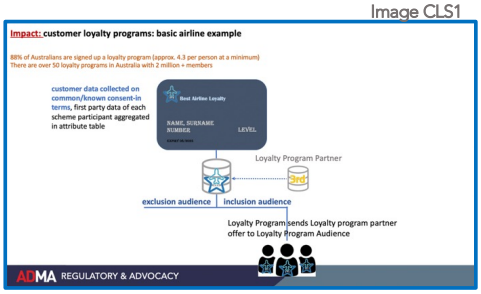
APPLICATION PAINTS A DIFFERENT PICTURE

The use case illustrations below were developed through consultations with digital marketers. The use cases are intended to assist evaluation of how Proposals would work in practice and thereby enable refinement of drafting and avoid unintended consequences.

USE CASE ILLUSTRATION 1: Complexities of Proposal 20

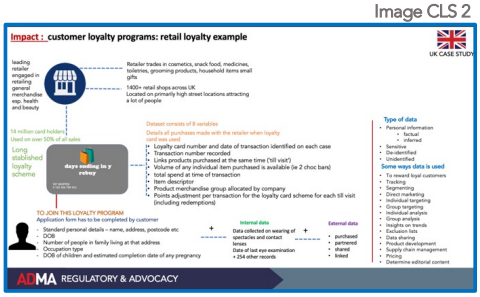
Images below are only included here for reference – ADMA welcomes the opportunity to discuss these in more depth with AGD.

Image CLS1



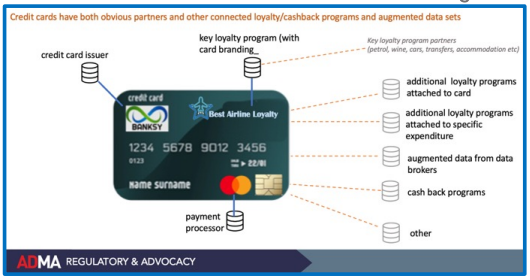
A single brand CLS – with data used to direct market to its own audience

Image CLS 2



A large retailer CLS, initial sign up and each engagement with the program builds inferred information into the profile, with the intention of direct marketing and targeting

Image CLS 3



A common example of a CLS where many programs are connected. Elements of each of image CLS 1 and 2 are part of the program – at scale across brands

Customer Loyalty Schemes (CLS) were one way of demonstrating everyday scenarios that could be impacted in different ways.

- Image CLS1, illustrated the practical situation of one brand, one audience and an easy way to opt-out
- Image CLS 2 focused on various ways inferred data is "collected" at each interaction to constantly enhance the user profile
- Image CLS3 is a complex but common CLS, where many different CLS programs are connected by the data subject at one time or another.

Of key concern to industry was how extending protections of the Act to de-identified information could have a flow on effect due to the interpretations of requirements under the Proposed laws.

Taking first the examples of the more basic forms of Customer Loyalty program (CLS1 and CLS2):

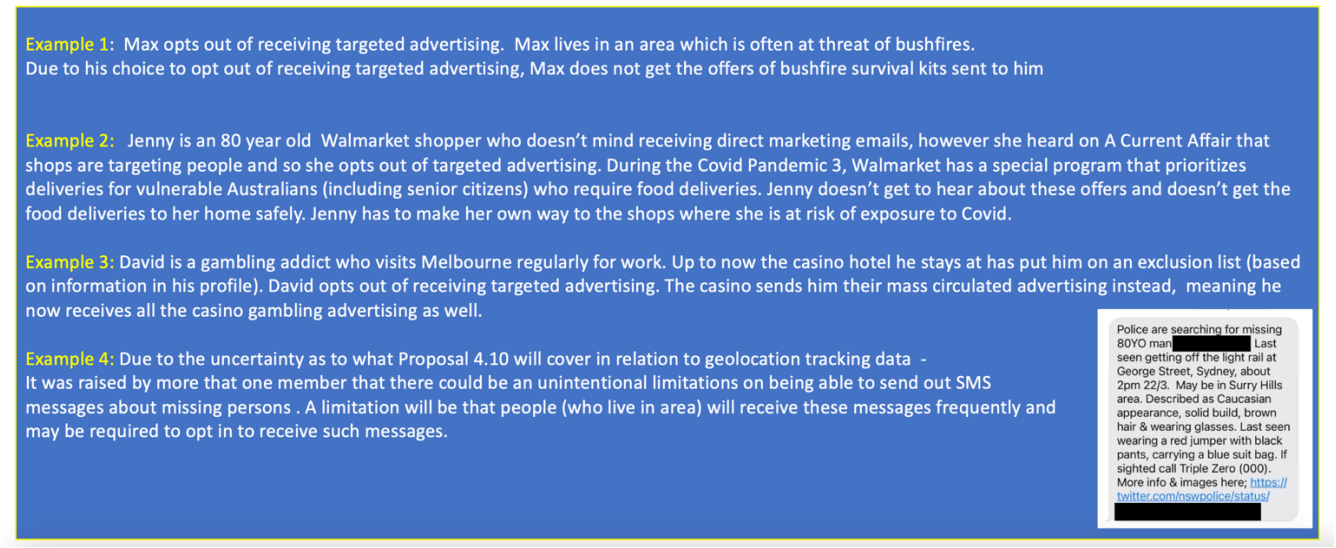
> **Basic Customer Loyalty Scheme:** *John Smith signs up to XYZ's loyalty program, provides personal information and asks to receive all benefits of the program. At time of joining, he is informed that personal information he provides, and information relating to him collected through his use of the program card and his interactions with program partners, will be used for personalised marketing. He is informed how information will be used for personalised marketing, and provided with the ability to use a preference centre to opt-out of particular forms of direct marketing and personalised marketing. Depending upon the scope and nature of preferences selected by John and the extent of John's interaction with the program, personalisation of offers may be limited (i.e., inclusion in broad audience*

segments for offer of a category of products of services based upon John's expressed interests or preferences or inference as to interests or preferences about people like John), more granular (i.e., exclusion from an audience segmented offer of a category of products of services based upon the program provider's knowledge that John already has that product or service), or differentiated for John or small cohorts of program customers that include John. John has had transparency and control of uses of personal information relating to him. He has a working understanding that when he uses his card, he will earn points and that offers are personalised based upon his interests or preferences, with the degree of personalisation affected by his selected preferences. John stays with the program if he continues to see value with it, although he may choose to opt out of particular forms of communication of offers (i.e., emails and/or text messages).

Applying the Proposals to this scenario , it is unclear as to the extent to which express upfront consent is required to enable this basic program participation. This basic program participation may be said to have elements within the high-level descriptions in the Report of each of Direct Marketing, Targeting, Trading in Personal Information and Automated Decision-Making. There is also a lack of clarity as to the extent to which consent (to the extent required) and ability to opt-out is required to be obtained and exercisable at the individual program participant level, or is able to be addressed at the program manager (XYZ) level. In relation to targeting, digital marketers questioned the level of detail required to be provided in 'informing' a consumer and how that could be done in the ways required of notices and policies. Also, what level of understanding a consumer must have to be able to make choices in relation to the use of their data and/or the choice to opt out of that data being used for targeted advertising?

USE CASE ILLUSTRATION 2: Targeting

The Proposal in relation to Targeting is not limited to activities generally regarded as advertising or marketing of products or services. This breadth of coverage may lead to adverse societal impacts.



Note: ADMA would welcome the opportunity to discuss with AGD other various use case scenarios as they were raised incorporating general examples that may impact all of industry in different ways.

5. Detailed explanation of ADMA's position in relation to Proposals

Part 1: Scope and Application of the Privacy Act

Objects of the Act – Proposal 3

i - OBJECTS OF THE ACT

In Proposal 3.2 it is recommended that the objects should be amended to recognise the public interest in protecting privacy:

ADMA broadly agrees with the proposal to amend Section 2A(b), but cautions against creating any uncertainty that could lead to an overly broad interpretation of "public interest".

OBJECTS OF THE ACT:

ADMA RESPONSE TO PROPOSAL 3.2:

In relation to Section 2A(b) and as outlined in response to the Discussion Paper ADMA believes a more appropriate formulation to be

'to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities to the extent that those functions and activities are consistent with benefit to Australian society'

Personal information, de-identification and sensitive information – Proposal 4

The definition of 'personal information' is a threshold legal concept that determines the boundaries of what is regulated and sought to be protected under the Privacy Act. It is therefore important that this definition is both flexible and platform/technology agnostic.

ii - LIST OF INFORMATION WHICH MAY BE PERSONAL INFORMATION

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

ADMA supports the objective of giving APP entities greater clarity in their evaluation of whether types of information may be "personal information that relates to an identified or a reasonably identifiable person".

Placing specific examples into the explanatory memorandum, or in OAIC guidance, rather than the statute itself, would allow for amendments to be made as technological development and change demands, without the need for amendments to the Act.

iii - COLLECTION REDEFINED TO COVER INFERRED/ GENERATED INFORMATION

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

Inferences that lead to accretion of information about an identifiable individual in a record held by an APP entity are already within the definition of personal information. The Report states that including 'inferred' in the definition of 'collect' removes confusion about when the APPs operate as to collection and use of inferred personal information, including in data analytics and machine learning processes: the collection would be stated to be at the point the inference is generated. ADMA supports implementation of this recommendation in relation to the point at which the inference is captured in a record held by an APP entity about (or in the new framework, relating to) an identifiable individual.

iv - REASONABLY IDENTIFIABLE SUPPORTED BY A LIST OF CIRCUMSTANCES

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

ADMA is concerned a reference list within the Act will prompt APPs to abandon the contextual evaluation that APP entities should continue to be required to undertake.

ADMA suggests if AGD moves forward with the recommendation that there be:

- a condition that links the list to a focus on the test in the definition; and
- that APPs are required to continue taking a contextual evaluation

Whether an individual is reasonably identifiable must be based on factors which are relevant to the context and circumstances in which the information exists. Given that the range of circumstances in which entities deal with information is broad and that each entity will need to conduct the assessment in their own context and address the reasonableness of identification in that context, having a non-exhaustive list of circumstances that an APP entity can refer to as a sense check seems appropriate . However, ADMA is of the opinion that such a list is better contained in explanatory notes and OAIC guidance than the Act.

v - AMEND DEFINITION OF 'DE-IDENTIFIED'

> *Proposal 4.5 recommends an amendment to the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context.*

In the era of big data, the debate over the definition of personal information, de-identification

and re-identification is an important one. Internationally, privacy regulations often rely on data being considered personal in order to require the application of privacy rights and protections. Data that is anonymous is considered free of privacy risk and available for public use.

Yet much data that is collected and used exists somewhere between these stages. Data identification is not binary, it lies on a spectrum with multiple shades of identifiability.

The Report states "De-identified information for the purposes of the principles-based Privacy Act should be defined to make it clear that de-identifying information is a process that involves it in such a way so as to not allow an individual to be reasonably identifiable while those circumstances persist".

The Report outlines the current definition in the Act mistakenly leaves an opening for de-identification to be considered a 'static' condition when it is not.

The Proposal makes sense in addressing that *de-identification instead be considered as 'a process, informed by best available practice, applied to PI that involves treating it in such a way that no individual is identifiable or reasonably identifiable in the current context.*

While adding in the "current context" does provide a guardrail within the definition, ADMA believes this is still too vague when you consider the environment in which de-identified information can be used.

For example in a data clean room/PET –data may be provided as de-identified but there is a chance that it may be re-identified depending on the other de-identified information provided. In this circumstance Proposal 4.5 doesn't provide clarity.

How far does "in the current context" apply? What impact would this then have in the case of targeting and the need to be able to provide an opt out of targeted advertising?

The language and application of the law around de-identified is critical. De-identified is a technique that protects privacy but also it allows aggregate data to be used and shared productively. Any reform to the current regulation needs to incentivise business to de-identify data where practicable to minimise risk exposure in the event of a cyber security breach. If there is no clear threshold within context, then it is possible that businesses will not bother to de-identify.

The GDPR explicitly recognises the intermediate level of de-identification with the concept of pseudonymous data.

'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

ADMA suggests that Australia take a similar approach to the GDPR when defining how the Act covers the process of de-identifying information.

vi - APP PROTECTIONS FOR DE-IDENTIFIED INFORMATION

As stated above, there are great benefits around de-identifying data including making it easier to share data with third parties. However it is important to note de-identification is not a guarantee that data is being processed fairly and ethically. Assessing the impact of the

processing is necessary to achieve that goal.

> *Proposal 4.6 recommends extending protections of the Privacy Act to de-identified information*
> *The recommendations in relation to APP11.1,*
> *require APP entities to take such steps as are reasonable in the circumstances to protect de-identified information:*
> *(a) from misuse, interference and loss; and*
> *(b) from unauthorised re-identification, access, modification or disclosure.*

ADMA supports this recommendation, once the definition of de-identified information is amended as mentioned above.

ADMA also recommends the introduction of OAIC guidance as to what is expected of a small compared to a large organisation in meeting this criteria. This distinction will help make the burden of compliance reasonably reflective of an organisations circumstances, including level of risk exposure and will help ensure the regulatory compliance (including systems) is not too burdensome for SMEs to manage if not required.

> *Proposal 4.6 recommends extending protections of the Privacy Act to de-identified information*
>
> *The recommendations in relation to APP 8, requiring APP entities when disclosing de-identified information overseas to take steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to de-identified information, including ensuring that the receiving entity does not re-identify the information or further disclose the information in such a way as to undermine the effectiveness of the de-identification.*
>
> *This recommendation again in essence makes sense however, even with this change, it is unlikely to eradicate the actual problem because what is "reasonably" able to directed by an APP entity is not necessarily the same as what is a practical outcome.*

ADMA is not opposed to this recommendation – but we don't believe it will have the desired impact.

vii - DE-IDENTIFIED INFORMATION IN RELATION TO TARGETING

> *Proposal 4.6 recommends the following extension of protections of the Privacy Act to de-identified information as it relates to Targeting - The proposed regulation of content tailored to individuals should apply to de-identified information to the extent that it is used in that act or practice.*

ADMA considers that if this recommendation were to be implemented as proposed there will be an unintended and highly problematic impact.

ADMA is concerned that the Report has put forward a concept of targeting that by its inclusion of 'de-identified information' will prove to be impractical for many 'entities carrying out their functions or activities to the extent that those functions and activities are consistent with benefit to Australian society'.

There are many societal benefits to data relating to citizens that depend upon the use of controlled and safeguarded 'data analytics environments' within which individual level (transaction and transactor) data may be linked and analysed. These environments have the appropriate level of data privacy and the assurance of security by design, for the purpose of handling data isolated within the controlled data environment, and releasing outputs from within

that control.

If an entity were to demonstrably (reliably and verifiably) disable itself from the capability to associate online data with an individual through technical means[3] and extract itself from environmental (contractual, operational and other) conditions (controls, safeguards and guardrails) such that individuals are no longer identifiable by any method reasonably likely to be used then that means the risk of harm to an individual of identification is sufficiently remote.

In this instance the information is and should be regarded as effectively or functionally de-identified and not be regulated as personal information (even with regard to targeting).

ADMA recommends not moving ahead with its Proposal 4.6 related to Targeting.

viii - GEOLOCATION TRACKING DATA

> *Proposal 4.10 recommends collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent and to define 'geolocation tracking data'.*

ADMA is concerned with the lack of clarity around location data and the definition of 'precision' and asks the Government to consider geolocation data in terms of when it relates to sensitive locations only. This would help relieve the large administrative burden of collecting consent.

This proposal will require more clarity, as tracking is an ongoing activity and geolocation data is a type of information.

When it comes to certain types of data, such as location, ADMA emphasises a need to consider the unintended consequences of a definition of 'geolocation tracking data' as personal information (and requiring consent).

As mentioned earlier in this submission, further, the absence of considering the abuse of location data means what may be considered sensitive national security locations e.g. Australian Parliament House, ADFA, Lucas Heights, etc. would all be reasonable to collect precise user location data on provided consent was provided.

ADMA is concerned that in the instance of geolocation targeting, the reliance of a consent framework is not always appropriate as, individuals are not adequately informed as to how their data will be used and any consent to such data use is therefore vitiated. ADMA believes that an "overarching test" as proposed (but measured by 'reasonableness') will be most effective in providing the necessary consumer protection.

This gets to the heart of what ADMA believes must be considered by regulators - that in most instances it's the potential (mis)use and/or abuse of the data itself that needs to be examined when developing new regulations, not simple broad definitions of categories and types of data.

ADMA recommends that geolocation tracking data as addressed in the Act be limited to sensitive locations

[3] "Means" could also include masking, anonymity, differential privacy, privacy- preserving machine learning, and synthetic data, as well as through data transformation such as aggregation).

PERSONAL INFORMATION, DE-IDENTIFIED INFORMATION

ADMA RESPONSE TO RECOMMENDATIONS:

Proposal 4.1 - ADMA supports replace the word 'about' with 'relates to' in the definition of personal information

Proposal 4.2 – ADMA recommends including a non-exhaustive list of information that may be personal information in the OAIC guidance – to facilitate evolution.

Proposal 4.3 – ADMA Supports amending the definition of "collects to expressly cover information obtained from any source including inferred information

Proposal 4.4 - ADMA suggests that if AGD moves forward with the recommendation that a non-exhaustive, list of information which may be personal information be provided, that each 'circumstance' requires a case by case contextual evaluation and to that end there be:

- a condition that links the list to a focus on the test in the definition; and
- APPs continue to be required to undertake a contextual evaluation.

Proposal 4.5 - ADMA recommends that the AGD consider the definition of 'de-identified information' to only relate to information reasonably capable of enabling identification when available in another context. Consider a similar approach to GDPR's 'pseudonymous data'

Proposal 4.6 – ADMA recommends that the AGD needs to tighten up the language in relation to applying some APPs to de-identified information or else there will be room for confusion in application. ADMA recommends that this application be only to information reasonably capable of enabling identification when available in another context, and then only for defined and limited contexts that do not include use in broad audience segments.

Proposal 4.6 - ADMA does not support the expansion of protections to de-identified information in relation to Targeting In this instance the information is and should be regarded as effectively or functionally anonymised (de-identified) and not to be regulated as personal information .

Proposal 4.10 - ADMA is concerned with the lack of clarity around location data and the definition of 'precision' and asks the Government to consider geolocation data in terms of when it relates to sensitive locations only

Small Business Exemption – Proposal 6

ix - SMALL BUSINESS EXEMPTION

ADMA represents many SME businesses that through their membership engagement have demonstrated commitment to responsible and accountable best practice in digital marketing and advertising. As ADMA mentioned in its response to the Discussion Paper[4], the principal issue for many SMEs is not a willingness to implement good data privacy practice, but as to their capabilities (technology systems, documentation of processes and practices, resources and knowhow) to implement compliance frameworks at the level required of APP entities. ADMA submits that SMEs need appropriate support, education and tools.

[4] Submission in response to AGD Privacy Act Review Discussion Paper, ADMA, page 13

For the reasons outlined in our submission in response to the Issues Paper[5] and Discussion Paper[6], ADMA continues to advocate that the removal of the small business exemption makes sense and believes that the Recommendations made in the Report are sensible with the right preparation, consultation and assessment as to Regulatory Impact. This work must be done by the government and industry to ensure that the burden of compliance is not unreasonable.
Through the past few years of the pandemic, Australia's SMEs have entered the data-driven digital economy faster than they ever expected and while this brings with it a level of responsibility, they need support, education and training to be able to comply.
ADMA supports the recommendations stated in the Report with the caveat that this cohort has compliance obligations introduced in a way that recognises their more limited capabilities[7]. The OAIC could be empowered to allow SMEs class exceptions or qualifications to particular requirements. The statute could include particular SME provisions, such as the Small Business Guide in Part 1.5 of the Corporations Act[8].
In addition to this support, a transitional period will be required.
In relation to helping to train this part of the community in best practice in privacy compliance, ADMA can be of assistance – offering a range of courses and training in this space.

SMALL BUSINESS EXEMPTION

ADMA RESPONSE TO PROPOSALS:

- **ADMA recommends that the small business exemption be removed. However, inclusion of SMEs in the data privacy statute should be done in a way that recognises their more limited capabilities.**
- **ADMA supports the OAIC being empowered to allow SMEs class exceptions or qualifications to particular requirements. The statute could include particular SME provisions, such as the Small Business Guide in Part 1.5 of the Corporations Act**
- **ADMA also recommends that an appropriate transition period be provided to aid with awareness of, and preparation for, compliance with the Privacy Act.**
- **ADMA supports the Government considering the provision of further resources for the OAIC, so it is well equipped to support this cohort.**
- **ADMA would also be prepared to work closely with the OAIC in helping educate, prepare and upskill SMEs through their ADMA Membership and/or through other ADMA education program where a course can be tailored specifically to aid small businesses with awareness of and preparation for compliance with the Privacy Act.**

Part 2: ProtectionsPrivacy policies and collection notices – Proposal 10 Consent and Online Privacy Settings – Proposal 11

x - PRIVACY SELF MANAGEMENT, TRANSPARENCY AND ABILITY TO WITHDRAW CONSENT

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

[5] Association for Data-driven Marketing and Advertising submission in response to the Privacy Act Review Issues paper 2020, page 13

[6] Submission in response to AGD Privacy Act Review Discussion Paper, ADMA, page 13

[7] limited capabilities" includes …educated personal, tools, tech architecture & ecosystem

[8] Corporation Act 2001 (Cth) – Part 1.5: Small Business Guide

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

Privacy policies must communicate information simply and clearly but with enough detail to be specific about their information handling practices. Today's data ecosystems are complex – with unprecedented types, forms, amounts and ways in which personal information is collected, shared, used and handled. This makes it challenging for an organisation to give clear information about the business's data handling practices.

Proposals 10.2 and 11.3 are important recommendations and while ADMA agrees with them, we also note neither of these proposals would be practicable or possible when put into practice alongside Proposal 19 and 20 – if they were to progress in this review as presented in the Report.

NOTICE & CONSENT

ADMA RESPONSE TO RECOMMENDATIONS:

Proposals 10.2 and 11.3 are important recommendations but ADMA neither of these proposals would be practicable or possible when put into practice if Proposal 19 and 20- were to progress in this review as presented in the Report.

FAIR AND REASONABLE TEST – Proposal 12

xi - FAIR AND REASONABLE TEST

ADMA advocates for individuals being able to take a certain level of data privacy safety for granted. ADMA agrees where a collection, use or disclosure of personal information is clearly and broadly harmful, the Privacy Act should prohibit that act or practice. It should not fall to the user to identify and avoid or mitigate that harm.

To that end, ADMA still very much supports the introduction of a threshold test that holds regulated entities to account, believing the right over-arching test will lift the level of data collection, use, handling, disclosure by an APP organisation and therefore the data-driven economy.

ADMA does **not** however believe the addition of the "fair and *reasonable*" test as outlined in proposal 12 of the Report, is the appropriate test. That test remains too subjective.

ADMA has concerns about each collection, use and disclosure having to meet ambiguous requirements of being both "fair" and "reasonable". In a Report that recommends that there should be a direct right of action of affected individuals (a recommendation which itself will open up floodgates to class actions), the "fair and reasonable" test leaves too much to interpretation.

ADMA supports the test as to 'reasonableness'. Unfair contract terms and misleading business practices should continue to be addressed by Australian Consumer Law. An affirmative obligation of 'fairness' is too subjective and likely to fuel plaintiff class action lawsuits.

Alternatively, ADMA recommends the AGD to consider suitability of the UK Data Protection and Digital Information (No. 2) Bill. This Bill was introduced to UK Parliament to provide a clear and business-friendly framework and approach to protecting individuals from privacy harms. This Bill recognises a list of activities considered to be 'legitimate interests'.

Legitimate interests is most likely to be an appropriate basis where you use data in ways people would reasonably expect and that have minimal privacy impact. Conversely, a business would

not be using data consistent with legitimate interests if they are using personal data in ways people do not understand and would not reasonably expect, or if the APP entity thinks some would object to if it were explained to them.

In Canada[9] the handling of personal information must be for a "purpose that a reasonable person would consider appropriate in the circumstances". Here the "reasonableness" is attributed to the individual to whom the personal information is related -while the "appropriateness" relates to the expected (legitimate interest) basis for the entity intending to process the data to provide the individual with the expected service, to the extent that those functions and activities are consistent with benefit to Australian society. This would mean that practices of concern, such as discriminatory behaviours, would be ruled out as they would not under any interpretation be considered "appropriate".

OVERIDING THRESHOLD TEST

ADMA RECOMMENDATION:

- **ADMA supports the *intention* behind an overarching threshold test which for individuals presents a stronger baseline protection against real and substantial concerns.**
- **ADMA does NOT support Proposal 12 in the form recommended ("Fair and reasonable") test as this test remains too subjective.**
- **ADMA supports test as to 'reasonableness'. Unfair contract terms and misleading business practices should continue to be addressed by Australian Consumer Law, An affirmative obligation of 'fairness' is too subjective and likely to fuel plaintiff class action lawsuits**
- **Alternatively ADMA recommends the Government further consider alternate options for a threshold test, perhaps looking to other data privacy regimes for possible alternatives such as the UK's Data Protection and Digital Information (No. 2) Bill.**

Rights of the individual – Proposal 18

xii - ERASURE

> *Proposal 18.3 Introduce a right to erasure with the following features:*
> *An individual may seek to exercise the right to erasure for any of their personal information.*
> *An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort.*
> *In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement.*

While in principal ADMA agrees with the intent of the erasure recommendation, consideration needs to be given where this 'right to erasure' could conflict with other statues, data retention rules and the need to keep a person on a suppression list, in order to ensure that their request to 'unsubscribe' from receiving commercial electronic messages is honoured.

[9] Department of Justice Canada – Privacy Act Modernisation: A discussion paper - "Privacy principles and modernized rules for a digital age" 29 December 2021 - Threshold for collection

RIGHT TO ERASURE

ADMA RECOMMENDATION:

ADMA supports the proposal outlining the right to Erasure with the following caveat: the Government engage in further consultation to consider what this would mean in application and how it will impact an APP entity's ability to comply with other regulations (such as the SPAM Act) and/or data retention rules.

AUTOMATED DECISION MAKING – Proposal 19

xiii - AUTOMATED DECISION MAKING

> *Proposal 19.1 Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights.*
> *Proposal 19.3 Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. Entities will be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similarly significant effect.*
> *This proposal should be implemented as part of the broader work to regulate AI and ADM, including the consultation being undertaken by the Department of Industry, Science and Resources.*

There is no doubt that Automated Decision Making (ADM) has become an increasingly prevalent facet of modern society both globally and within Australia, permeating both the public and private sphere, and filtering into an ever-expanding scope of individuals lives.

A scope of executive departments and agencies across Australia's federal jurisdictions utilise advanced computer systems to support government decision making — these include the Australian Taxation Office (ATO), Centrelink, the Department of Family and Community Services and the Australian Department of Defence[10]. Similarly, ADM systems are increasingly relied upon within the private sector. Of interest to ADMA members is Programmatic advertising - used by online platform operators in order to automatically generate advertising content based upon view data[11].

While greater transparency and explainability around automated decision-making makes sense, and will continue to make sense in the future, the language used in each of these recommendations is too vague, leaving room for bad actors to misuse the information.

Furthermore there is a danger that being required to provide *'meaningful information about how substantially automated decisions with legal or similarly significant effect are made' will have the unintended impact of:*

- *giving a blueprint to the bad actors to misuse the information they can learn about an APP entity's ADM;*
- not make a great difference to the individuals the reform was intended to protect; and/or
- could reveal commercially sensitive information with no privacy harm

[10] Administrative Review Council *Automated Assistance in Administrative Decision Making* Report No 46 (2004) p 57–63.

[11] Australian Competition and Consumer Commission (ACCC) *Digital Platforms Inquiry* Final Report (June 2019)

implications.

There is a balance that needs to be found in holding organisations accountable and remembering protection from privacy harm is paramount, but also understanding where risk of harm is not that great. Facilitation of a thriving competitive environment is desirable.

An alternative solution would be that the Regulator can, if required (and with good reason), request to check the ADM process being deployed by the organisation is reasonable. This shouldn't be a public free-for-all as that would be a huge red flag opening up gamification of the system by people knowing what triggers decisions. It would effectively be legislation that helps create a fraud manual for bad actors.

ADMA also questions how much of the information the average reasonable consumer would digest, if it were to be outlined in the APP Privacy policy and whether explainers would even be possible in a way that keeps the privacy policy 'clear, up-to date, concise and understandable' as is required in the recommendations in Proposal 10 of the Report.

Something further the Government should consider including is the GDPR 'off ramp' concept which highlights a right to a human intervention in decision-making processes if reasonably requested. It would not be unreasonable to expect companies be required to have processes in place in the event an automated decision is contested.

AUTOMATED DECISION MAKING

ADMA RESPONSE TO RECOMMENDATION:

- **ADMA supports greater transparency and explainability around automated decision-making where and in a way that makes sense.**
- **ADMA does NOT support the language used in each of these recommendation believing it to be too vague, leaving room for bad actors to misuse the information**
- **ADMA also supports a move for reform to include a right to human intervention in decision making processes if reasonably requested.**

Direct Marketing, Targeting and Trading – Proposal 20

xiv - DIRECT MARKETING DOES HAVE BENEFITS WHICH MUST BE CONSIDERED

ADMA is supportive of amendments to the way in which direct marketing is addressed in privacy reform so long as those reforms make sense. Also when considering the best approach to such reforms, the Government must not "fail to include in its assessment, the benefits of processing of data for direct marketing". Note for example: the FTT (First Tier Tribunal) found the ICO (Information Commissioners Office) had done just that in the case of *Experian Limited v The Information Commissioner* [2023] UKFTT 00132 (GRC).

Not all forms of direct marketing have a high privacy impact, even when delivered at scale. Therefore, ADMA advocates that, as the Privacy Review continues, the AGD continue to consider any reform and/or introduction of regulation in this space must appropriately distinguish between the more intrusive and covert tracking and profiling activities at one end of the scale,

and a business sending an email (or reasonably expected communication) to its existing customer base at the other.

xv - DEFINITION OF 'DIRECT MARKETING'

> *Proposal 20.1 (a) Amend the Act to introduce definitions for:*
> *Direct marketing – capture the collection, use or disclosure of personal information to communicate directly with an individual to promote advertising or marketing material.*

ADMA continues to advocate for a clear definition of Direct marketing to be included in the Privacy Act or the OAIC guidelines.

However, ADMA does not believe the definition as outlined in Proposal 20 is appropriately clear as there is room for it to overlap with the definition of targeting. If the definition of targeting is removed (or changed) the definition as drafted in the recommendation may be suitable.

In addition, ADMA suggests there is room for widespread education for APP entities and the community at large to better understand where direct marketing (as to the sending of communication directly to an individual) sits in relation to the Act. This will have particular assistance in helping APP entities better manage requests to withdraw consent, notify consumers of their right to object to the collection, use and disclosure of their personal information and when informing these individuals of such.

xvi - DIRECT MARKETING AND AN UNQUALIFIED RIGHT TO OBJECT

> *Proposal 20.2* ***recommends*** *providing individuals with an unqualified right to opt-out of their personal information being used of disclosed for direct marketing purposes*

ADMA recognises providing individuals with an "*unqualified* right to opt out," means APP entities would need to *stop*, not just take "reasonable steps to stop", the collection, use or disclosure of personal information for direct marketing purposes. This means that an entity would not be able to rely on any of the proposed exceptions to the right to object, to continue to use and disclose an individual's personal information for direct marketing. This approach does align with Article 21 of the GDPR and the UK GDPR.

However, ADMA believes the practical application of the revised Privacy Act, even with the proposed repeal of APP 7 being implemented, would have the same effect without needing to implement Proposal 20.2

The law would already, in practice, cover what it is hoping to achieve.

This Proposal (20.2) also appears to be similar to the existing requirement to provide an unsubscribe facility under the Spam Act. ADMA Members were keen to clarification as to whether Proposal 20.2 is intended to impose new process steps for APP entities to take, as this will be important for the purposes of any regulatory impact assessment. The AGD should clarify whether the proposed 'unqualified right to opt out' is intended to operate as a standalone process.

Interaction with Proposal 20.3

In addition, ADMA Members were keen for clarification as to what will be required in relation to the way the 'unqualified right to opt-out' relates to direct marketing and how that will interact with Proposal 20.3 – an 'unqualified right to opt-out' of receiving targeted advertising The Report indicates that these are intended to operate as separate, but overlapping opt-out mechanisms. Therefore, if an individual elects to opt out of targeted advertising but not direct marketing, an organisation will be able to continue to use personal information to communicate generic marketing, but not targeted advertising, to that individual. On the other hand, if an individual opts out of direct marketing from an organisation, this would—in most circumstances—automatically function as an opt-out from targeted advertising received directly from that organisation. ADMA members were keen to understand how to implement these Proposals and keep communication to customers clear and concise.

xvii - DIRECT MARKETING AND OTHER REGULATIONS

Further consideration will need to be given as to how any unqualified right to object would work alongside the SPAM Act, Do Not Call Register Act and a request to stop using an individual's data as consistent with the concept of a shared data right under Australia's Consumer Data Right.

xviii - INTRODUCTION OF DEFINITION OF TARGETING

> *Proposal 20.1 recommends introducing the following definition for Targeting - capture the collection, use or disclosure of information which relates to an individual including personal information, deidentified information, and unidentified information (internet history/tracking etc.) for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class).*

In order to clarify that targeting is distinct from direct marketing and uses a broader range of information relating to individuals, it is proposed targeting be defined in the Act to capture the collection, use or disclosure of information relating to an individual, including personal information, de-identified information and unidentified information.

ADMA also notes that the Act is fundamentally focused on the regulation of 'personal information'. Therefore the expansion of the Act to regulate behaviours and outcomes which do not relate to, or make use of, personal information would be inconsistent with its current objects.

ADMA does not support this definition of targeting being included in the Privacy Act. ADMA understands there is a need to address targeting intended to discriminate, create harm or is the result of malicious intent. However, including the recommended catch-all definition within the Privacy Act is unlikely to reduce the kind of activity that the government is hoping to abolish.

ADMA is concerned having such a broad definition of targeting as that outlined in the Report, will have implications with a domino effect in its triggering of other requirements within the Privacy Act/ Proposals. These are potentially far reaching and could have a negative impact overall.

Incorporating any/all segmentation into a definition of 'targeting', regardless of whether a person is identified/ reasonably identifiable, even where essential for operational or legal purposes and even when based on anonymous signals is not workable and could have unintended consequences.

The Proposals recommended in the Report are drawn from regulation introduced by the European Commission's Digital Services Act (DSA). The DSA is intended to address one of the most discussed topics connected to digital advertising – the prohibition of targeting minors. The DSA is aimed at ensuring a safe, predictable and trustworthy online environment by imposing certain obligations on intermediary service providers. The ultimate purpose of the DSA is to ensure intermediary service providers carry out proper content moderation. It does this by introducing significant obligations on online platform providers offering advertising on their interfaces.

In discussions with industry, ADMA has found wide-spread concern and confusion as to how and when any form of audience segmentation will remain practicable in data-driven and algorithmically enabled digital marketing. Most of this provides more benefits to society than the risk of harm.

Proposal 20.1 (Targeting) if taken forward would require substantial changes to existing business practices in targeted marketing and advertising. Therefore it needs to be an area of intense focus and discussion over the next few months. The AGD's proposals also go significantly further than any comparable jurisdiction.

Businesses already endeavouring to apply industry best practice in digital marketing have implemented clean rooms and privacy enhancing technologies to minimise risk exposure and continue to provide benefits that consumers have come to expect. If regulation like this is enacted, in essence there is a disincentive for industry to invest in user privacy enhancing technologies (PETs) and to minimise use of personal information and that actually sets up a negative incentive for good marketing.

Then there's the wider footprint beyond 'marketing' to be considered. The broad definition presented in the privacy review amendments includes the distribution of content, not just advertising. This will have an impact on content distribution that private business, platforms, publishers and government distributes. Advertising in and of itself will be impacted, but so too will the dissemination of any content that may (depending on the definition of targeted advertising) inadvertently be captured. Government campaigns designed to educate specific cohorts of people may unintentionally be included if it falls within a broad definition of "advertising" ('promotion' is often the word used to define advertising and that often catches more than is intended).

To try and eradicate what is the worst form of Targeting as intended, ADMA recommends the Government consider defining this kind of activity as "malicious targeting" so the correct guardrails can be implemented through the Privacy Act.

xix - TARGETING AND THE UNQUALIFIED RIGHT TO OPT OUT

> *Proposal 20.3 recommends providing individuals with an unqualified right to opt-out of receiving targeted advertising.*

The failure to define "targeted advertising" creates another level of uncertainty for compliance in relation to offering an unqualified right to opt out.

The modern targeted advertising ecosystem is complex and dynamic and is made up of actors playing different roles and serving different purposes. These actors can be distinguished into partially overlapping categories: marketers, publishers, and advertising intermediaries.

"Targeted advertising" unless otherwise defined, is considered to be a marketing practice that uses data about individuals to select and display ads or other forms of commercial content. It includes contextual advertising, based on the content of the webpages and keywords used in searches; segmented advertising, based on known characteristics of individuals; and behavioural advertising, based on observing behaviour. Without defining "targeted advertising" in the Act (the proposal is only for "targeting" to be defined), this wider definition will include some of the very forms of advertising that the Report points to as not being included (ie: contextual advertising).

Furthermore, if the definition of 'targeted advertising is a broad one, there would be instances where messaging that may be considered 'promotion' of a service may either be served to or withheld from a cohort an organisation was hoping to inform and/or avoid enticing with inappropriate communications.

Specific pillars of industry, including financial services, gambling and health, may need to meet other regulatory requirements to service products that are suitable by targeting messaging.

The entire purpose of advertising is to reach the customer that a message is relevant to. And consumers derive value in many ways from targeting practices. Targeting ought to be a legitimate interest. If the aim is to reduce the abuse of targeted information, such as discriminatory advertising like not showing jobs to certain audiences, then that is what needs to be regulated – not all of targeted advertising.

Just think about a billboard on a street that says "McDonalds Kiama is open for breakfast" near Kiama. How is this somehow less personal than a mobile phone ad targeting people in Kiama with the same message? Allowing people to opt-out of targeted advertising at more holistic level just reduces the relevance of the advertisements they receive. The result is a disparate advertising environment that actually encourages more invasive abusive as well as advertising that favours legacy players.

Competition is another consideration here. The large platform providers, which arguably have the most amount of data to serve targeted advertising, have the budgets and access to innovation that will allow them to find another way of continuing their business. It will be small businesses that end up crumbling under the burden of compliance and most limited by the restrictions brought about by needing to properly inform customers of their targeting advertising practices.

Advertising itself will continue to be served, even to the people who have opted out of targeted advertising. Advertising in itself is legal. All that will happen now is opted-out consumers will receive a 'firehose' worth of content that may or may not be relevant to them. The question the government needs to ask itself is whether this is the intended priority or focus of the privacy laws.

From a practical perspective, an organisation may only have de-identified data relating to a data subject. If this same data subject decides to 'opt out of targeted advertising, the request itself can't be fulfilled. The organisation would need to have an email address or phone number of that person in order to honour and record that request. Without that direct identifiable

information, the request to opt out would not be able to be recorded nor honoured. The administrative barrier alone deserves consideration before progressing with this Proposal.

Refining the definition of targeted advertising in order to allow people to opt-out will not necessarily stop the problem of targeted activity either. In the data protection domain, the idea that data subjects' self-determination may be effectively exercised through consent has been challenged by considering that meaningful consent is often impracticable, is subject to a power imbalance and fails to protect groups.

Providing the ability to opt out of advertising will absolutely reduce the number of messages people may find to be "creepy". Yet targeted advertising does provide multiple benefits for consumers as well as industry. It reduces costs for delivering effective ads to consumers with a strong appeal for the marketed products, while minimising ads "wasted" on non-interested consumers. Targeted advertising, carried out through computational devices, also makes it possible to monitor the effectiveness of advertising campaigns and, if needed, to tweak messaging. Content-based advertising is concerned not only with increasing sales, but also with creating and distributing valuable and enjoyable content, to attract audiences and build durable relationships. The benefit of targeted advertising also contributes to supply chain optimisation, lower prices for goods and services, access to free content/ services and more.

Another consideration is how an unqualified right to opt-out of targeted advertising will impact a business's ability to comply with other laws.
For example, a NSW resident opts out of receiving targeted advertising, and therefore the brand in honouring this request sends them an offer which is only redeemable in Victoria. While this is a bad customer experience, a bigger concern for the brand sending the offer is its failure to comply with Australian Consumer law (specifically section 18) relating to not sending material that could be deemed to be misleading or deceptive conduct by the brand.

For these reasons of uncertainty, ADMA suggests the government hold off on moving ahead with:

- its recommended definition of targeting and
- unqualified right for individuals to opt out of receiving targeted advertising.

Consultation with industry would help inform the Government on the practical impact including de-identified and unidentified information will have on the digital marketing economy vs the actual protection from privacy harms.

xx - INTRODUCING A DEFINITION FOR TRADING

> *Proposal 20.1 recommends amending the Act to introduce definitions for Trading – capture the disclosure of personal information for a benefit, service or advantage.*

As is the theme in the discussion of the recommendations in Proposal 20, there is a level of ambiguity that exists in this definition. This makes it difficult to support.

Page 210 of the Report outlines the definition of trading as above, then goes on to say that "the definition would be broader than the sale of information. For example, a company exchanging their customer list in return for that of another entity could constitute trading in personal information".

With this explanation, there was industry wide concern that customer loyalty programs would fall within this definition of 'trading'.

The concern is not about obtaining the necessary consent.The issue instead becomes about understanding how to provide customers with both the information required to comply and a method to opt out without unnecessarily confusing the customer and giving them a poor experience.

ADMA's further concern is, the broad definition of Trading appears to include any form of sharing of data or potentially even verification of data points with partner organisations or group members, consent requirements could become burdensome and place unnecessary onus on the individual.

In ADMA's discussion with industry, questions were raised as to whether the below examples were included in the broad definition:

- IDs shared within clean rooms for ID resolution/ data enrichment
- Unified solutions for ad targeting and measurement
- Automated data trading to third parties for core digital and e-commerce functions; and
- Data 'traded' between government departments.

ADMA recommends the definition of trading be clarified to remove uncertainty and that the AGD consult with Industry to better understand some use case scenarios for the purpose of ensuring regulatory development is practical and able to be applied to responsible business practices as they exist today. ADMA supports the definition to be clearly limited to the 'sale of information – with sale being defined expressly by a list of behaviours considered to be such). Furthermore the government could consult with industry to identify whether a list of what does not constitute 'trading' would be of benefit to help reduce any potential confusion.

xxi - REQUIREMENT THAT CONSENT BE OBTAINED TO TRADE PI

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

The proposal as to a consent- based framework for "trading in personal information" is not well explained, so it is very difficult to engage with in its current articulation. Its proposed boundaries are not explained. Do popular retail, airline, financial services and cross industry data partners "trade in personal information"? One would think not; however there is conflicting interpretation based on the AGD's proposals.

Clarification as to what trading is, would assist in ADMA determining its position as to the consent framework within which it is to operate. If the definition of trading of personal information is limited to the sale of information, then ADMA supports proposal 20.4

xxii - DIRECT MARKETING , TARGETING AND TRADING TO CHILDREN

Proposal 20.5 Prohibit direct marketing to a child unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests.
Proposal 20.6 Prohibit targeting to a child, with an exception for targeting that is in the child's best interests.
Proposal 20.7 Prohibit trading in the personal information of children.

ADMA supports proposal 20.5 to 20.7 on condition that the definitions of Direct Marketing, Targeting and Trading are more clearly defined as argued for above.

xxiii - INFORMATION ABOUT TARGETIING

Proposal 20.9 - Require entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals. Consideration should be given to how this proposal could be streamlined alongside the consultation being undertaken by the Department of Industry, Science and Resources.

It is ADMA's opinion that Australian consumers are not ready to receive this kind of information yet and doing so will provide a level of confusion that could create more problems than provide solutions. The market is not suitably mature enough.
This proposal is an overreach and is not demonstrating any consumer or commercial benefit.
ADMA appreciates that this proposal has been drafted with the intention of transparency, which is a key and important theme of this Review.
However, ADMA believes that rather than providing the protection to consumers, it will instead be provision of an instructional manual on how to commit fraud.
For example, assume the Australian Government was required to publish transparently on how automated systems made determinations if someone was flagged by immigration Once people know what causes one to get flagged, they would be able to just avoid the flags..

ADMA believes in its current form, this targeting approach is an overreach that doesn't manage the issue it intends to.

DIRECT MARKETING, TARGETING AND TRADING

ADMA RESPONSE TO RECOMMENDATIONS:

Proposal 20.1(a) – ADMA supports an inclusion of a definition of Direct Marketing but urges the government to consider avoiding the current overlap that will exist if the definition of targeting remains in the Act.

Proposal 20.1 (b) ADMA does not support the inclusion of the definition of "targeting" as outlined in the Report. Including de-identified and unidentified information in the definition makes the practical application too difficult, without the protections intended.

Proposal 20.1 (c) – ADMA recommends amending the definition of trading to be clearer. Not suitable in its proposed form. ADMA supports the definition to be clearly limited to the 'sale of information – with sale being defined expressly by a list of behaviours considered to be such).

Proposal 20.2 – ADMA supports the recommendation to allow for an unqualified opt out of Direct Marketing (so long as the definition of Direct Marketing is suitable defined for clarity as mentioned above).

Proposal 20.3 – ADMA does NOT support the consent framework proposed for Targeting. We believe it will put in place a huge compliance burden on business and would be confusing to consumers.

Proposal 20.4 – ADMA supports this proposal AFTER the definition of trading has been better defined to better align to the type of activity that relates to the sale of information.

Proposal 20.5 – 20.7 – ADMA supports the Proposals related to children once the definitions related to direct marketing, targeting and trading are updated to be clearer.

Proposal 20.9 – ADMA does NOT support the proposal around providing information about targeting.

ADMA strongly recommends that before proceeding with this Proposal, the AGD further consult with the digital marketing industry to discuss the practical implications and ways in which drafting can better mitigate the risks most of issue without creating an unnecessary compliance burden and/or confusion.

ENFORCEMENT - Proposal 25

xxiv - ENFORCEMENT – CIVIL PENALTY

Proposal 25.1 Create tiers of civil penalty provisions to allow for better targeted regulatory responses:

- *(a) Introduce a new mid-tier civil penalty provision to cover interferences with privacy without a 'serious' element, excluding the new low-level civil penalty provision.*
- *(b) Introduce a new low-level civil penalty provision for specific administrative breaches of the Act and APPs with attached infringement notice powers for the Information Commissioner with set penalties.*

ADMA supports this proposal but recommends that the government include a consideration to the size of business in determining enforcement tiers and penalties. This is to ensure that SMEs are not unfairly exposed to the most severe fines ($50million +).

ENFORCEMENT – CIVIL PENALTY TIERS

ADMA RESPONSE TO RECOMMENDATIONS:

Proposal 25.1 – ADMA supports the proposal to create tiers of civil penalty provisions to allow for better target regulatory responses, but ADMA recommends that an inclusion to consider the size of the business is needed to ensure severity of fines/ penalty is proportionate for SMEs.

A DIRECT RIGHT OF ACTION – Proposal 26

xxv - A DIRECT RIGHT OF ACTION

Proposal 26.1 Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy. The model should incorporate the appropriate design elements discussed in this chapter.

This proposal, when coupled with developing law, will be of some concern to APP entities and their insurers as to new litigation risks and financial liabilities. Plaintiff class action law firms will likely potentially warmly embrace this proposal. Care needs to be taken to ensure APP entities are not subjected to unreasonable litigation (both individual and class action).

The drafting of the final proposal in relation to this needs to avoid a situation where the Privacy Commissioner would cease to be the gatekeeper to the Courts in relation to infringements of the Privacy Act. While this reduce any increase in pressure on resources of the Privacy Commissioner, the new right needs to be carefully thought and circumscribed to ensure that it is fit for purpose[12].

A direct right of action that is not well thought through risks the Americanisation of the legal system. This will increase risk and expense for all businesses, and add complexity to the data landscape - litigation on *perceived grievances*. However, an effective path for Australia to take could be to model after GDPR where a regulator has investigative and punitive capability.

ADMA recommends this Proposal be considered more thoroughly both in terms of impact on the Regulator authority and increased burden on APP entities (costs of insurance shouldn't be disregarded in the analysis

A DIRECT RIGHT OF ACTION
ADMA RESPONSE TO RECOMMENDATIONS: **Proposal 26.1 – ADMA supports but with further consultation to guardrail the Privacy Commissioners role as gatekeeper to the Courts and also to limit APPs exposure to unreasonable litigation (and by extent- associated costs).**

[12] Peter Leonard Recommendations Privacy Act, February 2023, Data Synergies Pty Ltd,

7. OTHER RECOMMENDATIONS

CUSTOMER LOYALTY SCHEMES

ADMA recommends that the AGD give more clarification with respect to customer loyalty schemes. There was reference to "most submissions generally took the view that customer loyalty schemes should not be regulated differently or separately". There was however no clarification as to how the AGD did contemplate they ought to be considered.

The positioning of customer loyalty schemes within the section of the Report dedicated to trading, could lead one to think this is how the AGD considers the way customer loyalty schemes operate, but confirmation of the intention – either way would be beneficial.

If Customer Loyalty Schemes (CLS) are required to allow people to opt out of target marketing (and not condition the provision of services to targeted marketing) then the value proposition of Customer Loyalty Schemes, delivery of service becomes fraught. CLS, help keep prices down, improve supply chain efficiency and optimisation and provides customers with offers and content of interest and value.
It is clear Australians see value in participating in Customer Loyalty Schemes, with 88% of Australians being signed up to a loyalty program[13]
If such programs were to be considered to be trading in information, it is most likely to be the SME businesses that will suffer the most.

REGULATORY SANDBOX

The Report showed a very clear intention of the Government to ensure that the Privacy Act moves towards building Australia's digital trustworthiness.

Regulators internationally are giving focus on Privacy Enhancing technologies to allow businesses to optimise the benefits that sharing data can bring while also protecting the individual from any privacy harms.

A growing number of policy makers and privacy enforcement authorities are considering how to incorporate PETs in their domestic privacy and data protection frameworks. However the highly technical and fast evolving nature of these technologies often presents a barrier to implementation by organisations and to their consideration in policy and legal frameworks applicable to data.

Organisations need to find ways in which to use de-identified information safely and securely. A wide variety of policy initiatives on PETs is underway across OECD countries. Other jurisdictions are promoting innovation in and with PETs through a range of initiatives including regulatory sandboxes[14].

---

[13] For Love of Money 2022 – The Point of Loyalty Survey 2022 (10th Edition)

[14] Emerging Privacy Enhancing Technologies – Current Regulatory and Policy Approaches – OECD Digital Economy Papers March 2023, No 351, Page 33

Examples such as the Singapore government's Digital Trust Centre- that is leading research and development of trust technologies and supporting talent development in this space. For Australia to build a similar digital trustworthiness, it would be beneficial to consider developing a similar investment in supporting development and upskilling in this space.

ADMA recommends investing in both research, development, upskilling in this place while at the same time considering a framework within which participants can test, innovative concepts in the market under relaxed regulatory requirements at a smaller scale, on a time-limited basis and with appropriate safe guards in place.

Doing such will foster the principle of learning by doing, helping to identify and escalate problems in a 'real' environment. This will strengthen the likelihood of developing a Privacy regime that is fit-for-purpose. A regulatory sandbox will also give businesses the opportunity to test product viability while ensuring better outcomes for consumers. It also supports innovation and provides an environment that allows government the opportunity to learn and see the impact certain recommendations may have in application.

PRIVACY VERSUS DATA BREACHES

As this process of review continues there is also a need for more education in this space to distinguish between data breaches and privacy considerations. There has been a lot of concern recently from headlines in the media around recent large data breaches from some of Australia's largest companies. Each of these headlines get painted with the "privacy brush", but it would be good to remind the market and the media there is a difference between a data breach (loss of, unauthorised access to or unauthorised disclosure of personal information) and a privacy breach (which, although not a defined term typically means any conduct which breaches one or more APP). Therefore, it is possible for a breach to be a data breach, but not necessarily a privacy breach – and vice versa.

This education is imperative to remind everyone the answers don't all lie in the review of the Act alone – in fact much of the harms can be managed through best practice.

8. ABOUT ADMA

ADMA represents the full 360 degrees of Australia's media, marketing and advertising ecosystem. ADMA itself is the principal industry body for data-driven marketing and advertising in Australia, representing over 350 organisations from a broad spectrum of Australian industries. Together these organisations employ about 28,000 marketing professionals, many of whom are on the cutting edge of the data revolution. Members range in size from SMEs to multinational corporations. They include banks and telecommunication companies, global tech companies, advertising agencies, specialist suppliers of marketing services, statutory corporations, retailers, specialist industries such as travel, hospitality and automotive, charities (both large & small) and educational institutions.

ADMA, as the principal industry body for data-driven marketing and advertising, is committed to upholding good standards in data privacy. ADMA members are advocates of responsible marketing and as such recognise that a sustainable marketing and advertising sector requires fair and transparent business practices in the handling of consumer data (including personal information) and that such practices reflect a respect of consumers which in turn nurtures digital trust.

ADMA acknowledges that our members may have an interest in individual questions raised in the Issues Paper, however in this submission we focus on key issues as they pertain to the data-driven marketing and advertising industry.

Individual members of ADMA may provide separate submissions to the Attorney-Generals Department.