ADMA Association for data-driven marketing & advertising

Submission in response to the Privacy Act Review – Discussion Paper, October 2021

Australian Government, Attorney- General's Department

30 January 2022

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

ADMA
Intelligent Marketing

Table of Contents

INTRODUCTION 3

GENERAL COMMENTS 4

1. OBJECTS OF THE ACT 6

2. DEFINITION OF PERSONAL INFORMATION 7

4. SMALL BUSINESS EXEMPTION 13

8. NOTICE OF COLLECTION OF PERSONAL INFORMATION 15

9. CONSENT TO COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION 15

10 – ADDITIONAL PROTECTIONS FOR COLLECTION, USE AND DISCLOSURE 21

14 – RIGHT TO OBJECT AND PORTABILITY 26

16 – DIRECT MARKETING, TARGETED ADVERTISING AND PROFILING 27

21. CONTROLLERS AND PROCESSORS OF PERSONAL INFORMATION 33

22. OVERSEAS DATA FLOW 34

CONCLUSION 35

ABOUT ADMA 36

ADMA
Intelligent Marketing

Introduction

The Association for Data-driven Marketing and Advertising (**ADMA**) welcomes the opportunity to make a submission to the Attorney-General's Department (**AGD**) in relation to the Privacy Act 1998 (Cth) Review Discussion Paper October 2021 (**Discussion Paper**).

The Australian Government's Review of the Privacy Act 1988 (**Review**) aims to ensure that Australia's data privacy framework empowers individuals through the protection of data relating to them, and that it does so in a way that best serves Australian society. ADMA considers this to be a very important legislative review. Consumers benefit from both privacy protection and engagement in the digital economy. Our members support a data privacy regulatory framework that protects personal information, while accommodating respectful and fair collection and use of customer data.

This Review provides the opportunity, through legislature reform, to *address uncertainties* that exist in the interpretation and operation of the Privacy Act; to provide *additional protections* as appropriate to reduce risk of privacy harms to individuals; to consider how to *improve overseas cross data flows* by minimising friction without sacrificing security; and to ensure *improvement of the overall* level of privacy protection and trust that Australian society has in today's data-driven, digital economy.

In order to operate effectively for all and promote innovation and growth, **the Review will need to determine whether Australia's privacy regime is fit for purpose in:**

- protecting consumers from individual and collective privacy risks and harms;
- providing appropriate transparency as to how and why organisations use and disclose the data they hold and access;
- empowering consumers to control uses and disclosures of personal information beyond those that are a reasonable incident of [provision of a product or service;
- making organisations more accountable in their data handling processes and practices;
- providing confidence that the digital economy operates in line with community expectations and within clear boundaries;
- establishing a future-proof regulatory environment that is flexible enough to support competitiveness and innovation, while also being robust enough to set guardrails that support proactive and targeted regulation, strategic enforcement and that serves as a general deterrent to mishandling of personal information;
- staying relevant to the requirements of Australian society while also supporting global interoperability, through a consistency of protection and safeguard of, as necessary, domestic and cross-border personal information flow; and
- aligning with evolving best practice in coverage and effect of national data privacy (data protection) statutes, and statutes regulating automated decision making, thereby reducing friction for Australian businesses expanding overseas and in cross-border transactions, and future proofing the statute to the extent reasonably practicable.

International Learnings: Australia has the opportunity to select and tailor the best features of new data privacy statutes from around the world as it overhauls Australia's Privacy Act[1] to bring it to the standard required for a thriving data-driven digital society.

Data-driven marketing and privacy reform: ADMA represents the data-driven marketing and advertising sector in Australia. This dynamic sector is a substantial contributor to the Australian economy. Through ad-supported services, this sector facilitates low cost or free access to content and information, and better prices for products and services across many sectors of the Australian economy. Many ADMA member organisations have invested heavily in technology, training and education to align data privacy practices with evolving regulator expectations as to data privacy governance and assurance and privacy enhancing processes and practices. Targeted advertising is not welcomed by some consumers, but may enjoy more relevant ad content and free or ad subsidised services, and offerings and other consumer benefits. Targeted advertising also reduces costs to reach potential buyers, lowering barriers to entry for SME businesses. Throughout this Review, ADMA places the protection of individuals from the more serious privacy harm[2] at its focus, when considering the need for legislative reform of the Privacy Act to address acts and practices of APP entities that cause privacy harms[3]. Properly governed and data privacy assured target advertising does not lead to privacy harms. ADMA supports legislative reforms that provide appropriate incentives (and possible sanctions) for good governance and assurance of collection and handling of personal information relating to individuals. This submission addresses reforms that ADMA considers are consistent with a statutory focus upon addressing privacy harms and improving responsibility and accountability of APP entities.

General Comments

Data privacy law is a critical component of an economy enabled by data and data analytics. Handling of consumer data is a necessary incident of conducting online business. Consumer trust and participation is critical for a vibrant digital economy. The process of regulatory reform needs to identify how data privacy reform can; improve efficiencies and benefits to consumers, maintain digital trust, provide regulators with appropriate authority, ensure businesses are accountable for poor data privacy governance, and assurance, and transparent, and responsible in handling of personal information , while minimising regulatory and compliance burdens.

---

[1] Peter Leonard, Data privacy, fairness and privacy harms in an algorithm and AI enabled world, January 2022 (This paper was Data Synergies submission in response to the AGD Review of the Privacy Act 1988, Discussion Paper)

[2] Possible 'privacy harms' include inconvenience or expenditure of time; a negative outcome or decision with respect to an individual's eligibility for a right, privilege or benefit such as related to employment, credit, insurance, government assistance, certification of licences, including denial of an application, obtaining less favourabe terms, cancellation, or an unfavourable change in terms, online abuse,, discrimination, stigmatisation or reputational injury, disruption and intrusion from unwanted communications or contacts and other detrimental or negative consequences that affect an individual's private life, privacy affairs, private family matters or similar concerns.

[3] Possible 'privacy harms' include inconvenience or expenditure of time; a negative outcome or decision with respect to an individual's eligibility for a right, privilege or benefit such as related to employment, credit, insurance, government assistance, certification of licences, including denial of an application, obtaining less favourabe terms, cancellation, or an unfavourable change in terms, online abuse,, discrimination, stigmatisation or reputational injury, disruption and intrusion from unwanted communications or contacts and other detrimental or negative consequences that affect an individual's private life, privacy affairs, private family matters or similar concerns.

Reform only where needed: Data privacy reform should focus upon mitigation of risks of privacy harms, without causing unreasonable costs to businesses as may arise through new regulation addressing unlikely or exceptional circumstances or impeding innovation, efficiency and consumer benefit.

"The moves to protect privacy need to be careful not to entrench the power of incumbents who have the means (technical, financial and legal) to be legally compliant while circumventing the spirit and intent of the laws"[4].

Reform of a data privacy statute is complex. Expanding legal principles-based requirements readily leads to unintended consequences, given speed and unpredictability of technological change and innovation in data analytics processes and practices. Reforms should address known concerns as to acts and practice causing privacy harms, not hypotheticals.

A Privacy Act for today and the future: Many of the gaps that exist in the current regulatory framework lie in the drafting of legislation designed for a landscape that existed before the advent of the internet and other technological innovations that facilitated the proliferation of data and information. While the Act was drafted to be 'technology neutral', advances in technologies created concepts, processes, identifiers and platforms that the Act does not clearly address. As a consequence, there is uncertainty in application of the Act to some acts and practices that carry unacceptable risks of privacy harms. Some APP entities take advantage of that uncertainty. Creation of certainty in addressing known concerns as to acts and practices causing privacy harms should not be at the expense of future innovations. Caution should be exercised to avoid applying too tightly the clarity of today to the possibilities of tomorrow.

ADMA's recommendations address the following:

- The Objectives of the Privacy Act
- The definition of personal information
- The small business exemption
- Notice
- Consent
- Additional protections for collection, use and disclosure
- Right to object and portability
- Direct marketing, targeted advertising and profiling
- Controllers and processors of personal information
- Overseas data flows

[4] Joshua Lowcock, Mi3 podcast "Media execs: ACCC risks strengthening big techs dominance without first tackling privacy, February 2021

Part 1: Scope and Application of the Privacy Act

1. Objects of the Act

Proposal 1.1:
Amend the objects in section 2A, to clarify the Acts scope and introduce the concept of public interest as follows:

a) *To promote the protection of the privacy of individuals with regard to their personal information; and*
b) *To recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities undertaken in the public interest*

The Objects should make clear that interests of an individual in relation to handling of personal information relating to them is legally protected. ADMA proposes that Section 2A(a) should read:

(a) *"To promote the right for individuals to the protection of personal information relating to them".*

The AGD proposes that Section 2A (b) should introduce the concept of public interest as follows:

(a) '*to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities undertaken in the public interest* '

ADMA broadly agrees with the proposal to amend Section 2A(b), but submits that the proposed wording *"activities undertaken in the public interest"* creates uncertainty that could lead to an overly broad interpretation of "public interest".

ADMA suggests a more appropriate formulation of Section 2A(b) might 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'*

OBJECTS OF THE ACT:

ADMA RECOMMENDATIONS:
Amend the first Object in Section 2A(a) *to read:*

"To promote the right for individuals to the protection of personal information relating to them"

In relation to Section 2A(b) 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'*

ADMA
Intelligent Marketing

2. Definition of personal information

Proposals 2.1-2.5:

- *Change the word 'about' in the definition of personal information to 'relates to';*
- *Include a non-exhaustive list of the types of information capable of being covered by the definition of personal information;*
- *Define 'reasonably identifiable' to cover circumstances in which an individual could be identified, directly or indirectly. Include a list of factors to support this assessment;*
- *Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information; and*
- *Require personal information to be anonymous before it is no longer protected by the Act.*

The effect of proposals 2.1- 2.3 would be that the definition of 'personal information' would become:

'*Personal information means information or an opinion that relates to an identified individual, or an individual who is reasonably identifiable:*

(a) Whether the information or opinion is true or not; and

(b) Whether the information of opinion is recorded in a material form or not.

An individual is 'reasonably identifiable' if they are capable of being identified, directly or indirectly.

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.

> *"Understanding the scope of what is meant by 'personal information' – and ensuring that that definition remains fit for purpose – is a critical endeavour in privacy jurisprudence"*[5].

ADMA welcomes and supports the AGD's intention to modernise the definition of personal information to ensure that it remains relevant in a digital economy, interoperable with relevant domestic laws and comparable international data privacy jurisdictions.

There are varying impacts to each of the proposals put forward to 'improve' the definition of personal information and each need to be considered in both isolation and collaboratively to ensure that any amendment improves the definition rather than make it more convoluted or abstract.

CHANGING WORDS IN THE DEFINITION OF PERSONAL INFORMATION

Proposal 2.1 recommends changing the word 'about' to instead read as 'relates to'.

This will broaden the circumstances in which information is covered by the Privacy Act. While this may, at the surface be disfavoured by some, the change will provide more clarity for APP entities

[5] See https://www.salingerprivacy.com.au/wp-content/uploads/2020/11/20-11-20_Privacy-Act-review_Salinger-Privacy_Submission.pdf

in understanding the way they are expected to operate in their handling of such information. ADMA recognises that the responsible marketer, more often than not, has the right intentions as to handling the personal information they hold, in a compliant manner, but often faces unsurety as to whether information is classified as personal information or not. The removal of doubt will make the framework for compliance clearer and reduce mishandling of information.

Current uncertainty in interpretation of the term 'about' reflects the gap between the reasoning of the Full Federal Court in the Grubb case[6] and the current wording of the Act. There is an opportunity in this Review to bring closer alignment between the Commissioner's current guidance[7] and the words of the Act.

The ACCC in its Digital Platforms Inquiry Final Report stated the following:
"*there are significant benefits in updating the definition of 'personal information' so that it covers the realities of how data is collected on individuals in the digital economy and to bring the Australian privacy regime into greater alignment with standards set by overseas data protection regulations.*"

ADMA supports proposal 2.1 on the basis that the amendment would ***partially*** clarify coverage of technical data, in line with the ACCCs recommendations.

The implementation of Proposal 2.1 will also promote interoperability with comparable definitions locally (ie the Consumer Data Right (**CDR**), as well as internationally, with the EU General Data Protection Regulation (**GDPR**), South Africa's Protection of Personal Information Act[8] (**POPIA**), and comparable statues by relevant regulators.

CONTEXTUAL EVALUATION REMAINS IMPORTANT

ADMA submits that any change in wording should not bring about a fundamental shift in the requirement to make a contextual evaluation when determining if technical data should be considered to be 'personal information'.

There should be a continuing requirement to take into account:

- the nature of the information;
- the data environment in which that information is held and managed; and
- the availability of other potentially identifying information (held in that data environment) where it is reasonably practicable to associate the information with an identifiable individual.

[6] Privacy Commissioner v Telstra Corporation Ltd [2017] FCAFC 4 (**Grubb Case**)
[7] https://www.oaic.gov.au/updates/news-and-media/privacy-commissioner-v-telstra-corporation-limited-federal-court-decision
[8] Protection of Personal Information Act July 2020, South Africa

The revised Privacy Act, or associated explanatory material, should make it clear that this contextual evaluation continues to be, and is, required.

Any assessment must consider the particular circumstances of that entity and that entity's reasonable access to other information, the nature of the relevant information and the data situation in which that relevant information is collected and handled. Determination of whether particular types of technical information can be considered 'personally identifiable' depends upon other, potentially identifying, information relating to an individual reasonably available to a particular APP entity.

LIST OF TYPES OF INFORMATION CONSIDERED TO BE PERSONAL INFORMATION

- *Proposal 2.2 recommends the inclusion of a non-exhaustive list of the types of information capable of being covered by the definition of personal information.*

ADMA notes the objective of providing greater clarity for APP entities in evaluation of whether types of information may be personally identifying. However, ADMA submits that inclusion of a list risks creating confusion as to the contextual evaluation that APP entities should continue to be required to undertake.

The example list of technical information provided in the Discussion Paper[9] largely mirrors the list of identifiers in the definition of personal data in the GDPR. However, the GDPR provides this list not to specify items on the list as personal data, but rather to illustrate that personal data may include any information relating to an identified or identifiable natural person'. Assessment is required as to whether in a particular context items on the list are identifying.

ADMA suggests that if AGD proposes to move forward with a recommendation that an illustrative, non-exhaustive, list of technical data is provided, the recommendation is for this list to be in the explanatory memorandum, or OAIC guidance, rather than the legislation itself. Amendments to guidance can be made as technological development and change demands, without the need for amendments to the Act.

INFERRED OR GENERATED INFORMATION

Proposal 2.4 suggests that the definition of collection be 'amended to expressly cover information obtained from any source and by any means, including inferred or generated information'.

The definition of personal information already contemplates inferences by addressing 'opinions', 'whether true or not' about an individual[10].

[9] AGD, Privacy Act Review Discussion Paper, October 2021, page 27
[10] AGD, Privacy Act Review Discussion Paper, October 2021, page 24

The Discussion Paper suggests that 'APP entities may find it difficult to practically determine the point at which opinions or inferences they generate become personal information'[11]. The amendment would not reduce this difficulty, although it may address any uncertainty as to whether "collection" encompasses creation of identifiability through ability of an APP entity to infer identity (for example, by mosaic or pattern analysis of multiple data points relating to an individual), even if relevant data points in the form received by an APP entity were not of themselves identifying. "Collection" might reasonably include the act or practice of generating or inferring information.

ANONYMISATION

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

The Discussion Paper proposes an amendment to the Act, to require information to be 'anonymous' rather than 'de-identified' for the Act to no longer apply.

ADMA is concerned that the Discussion Paper advocates a concept of anonymisation that in practice is likely to be unattainable for many '*entities carrying out their functions or activities to the extent that those functions and activities are consistent with benefit to Australian society*'.

The standard of anonymisation is too high, especially if personal information is expanded to include technical data. Anonymisation (or destruction) of technical information (including communication metadata) which is not retained or used in the way that an individual would be identified in the ordinary functions of an APP entity would create huge compliance burdens for the industry with little or no discernible privacy benefit for the consumer.

Furthermore, 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.

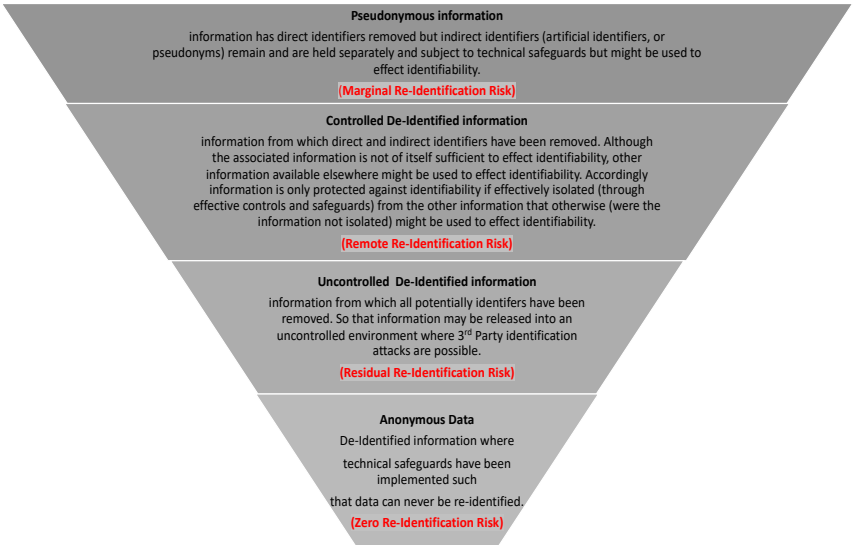
If an entity were to demonstrably (reliably and verifiably) disable itself from the capability to associate online data with an individual through technical means[12] and extract itself from environmental (contractual, operational and other) conditions (controls, safeguards and guardrails) such that individuals are no longer identifiable by any method reasonably likely to be used then that means that the risk of harm to an individual of identification is sufficiently remote.

[11] AGD, Privacy Act Review Discussion Paper, October 2021, page 24

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

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.

"De-identification" as a term, is commonly used and can sit anywhere along below spectrum outlined below:



COMPLETE ANONYMISATION IS NOT POSSIBLE

In practice it cannot be guaranteed that most consumer data is anonymised to the point where over time re-identification is impossible[13]. This is because other data sources may become available that facilitate mosaic identification attacks or technical processes for identification attacks in ways that cannot be reasonably anticipated by a regulated entity. For this reason, state of the art analyses of anonymisation technologies and techniques draw a clear distinction between functional anonymisation (effective anonymisation) and complete anonymisation (full anonymisation)[14].

Many experts consider that complete and (full) anonymisation is not possible in practice for most consumer data[15].

The Anonymisation Decision-Making Framework: European Practitioners' Guide[16] outlined the following consideration of complete anonymisation and functional anonymisation:

[13] Luc Rocher, Julien M Henrickx & Yves-Alexandre de Montjoye "Estimating the success of re-identification in incomplete datasets using generative models", July 2019
[14] Peter Leonard, Data privacy, fairness and privacy harms in an algorithm and AI enable world, January 2022 (This paper was Data Synergies submission in response to the AGD Review of the Privacy Act 1988, Discussion Paper)
[15] Luc Rocher, Julien M Henrickx & Yves-Alexandre de Montjoye "Estimating the success of re-identification in incomplete datasets using generative models", July 2019
[16] Mark Elliot, Elaine Mackey and Kieron O'Hara The Anonymisation Decision-Making Framework: European Practitioners' Guide page 10

A common error when thinking about anonymisation is to focus on a fixed end-state of the data. This is a problem because it leads to much muddled thinking about what it means to produce 'anonymised data'. Firstly, it focuses exclusively on the properties of the data whereas in reality the anonymity or otherwise of data is a function of both the data and their context. Secondly, it leads one into some odd discussions about the relationship between anonymisation and its companion concept risk, with some commentators erroneously (or over-optimistically) assuming that anonymity entails zero risk of an individual's being re-identified within a dataset. Thirdly, viewing it as an end-state means that one might assume that one's work is done once the anonymisation process is complete and the end- state is produced, which in turn promotes a counterproductive mentality of 'release-and-forget'.
In many ways, it would be better to drop the adjectival form 'anonymised' altogether and perhaps talk instead of 'data that have been through an anonymisation process'…, we will use the term 'anonymised' but this should be understood in the spirit of the term 'reinforced' within 'reinforced concrete'. We do not expect reinforced concrete to be indestructible, but we do expect that a structure made out of the stuff will have a negligible risk of collapsing.

On the other hand, functional anonymisation does not assume that anonymisation can be zero-risk or irreversible; it is meant instead to bring anonymisation practice in line with the art of the possible, in particular by understanding that whether data are or are not anonymised is not a property of the data, but determined by the relationship between the data and the context(s) in which they are held. Given that, it is clear that risk cannot be totally eliminated, but rather we work to reduce the risk of re- identification of individuals from functionally anonymised data to a negligible level.

If anonymisation is to replace de-identified as the relevant term in the statute as proposed in the Discussion Paper, it needs to be clear that the standard remains 'functional' anonymisation where individuals are not identifiable by any means reasonably likely to be used. That is, the test will be that the risk of re-identification would be sufficiently remote as compared to full anonymisation (where individuals cannot be identified by any conceivable means).

ADMA does not support an interpretation of anonymised to be a requirement for APP entities to irreversibly anonymise information to meet the threshold of 'extremely remote or hypothetical (as outlined in the Discussion Paper).

DEFINITION OF PERSONAL INFORMATION

ADMA RECOMMENDATION:

- the definition of personal information should be changed to:
  - replace the word '*about*' with '*relates to*'
  - add "*Includes information or opinion which has been created, generated or inferred*" (if express clarification is required)

- The revised Privacy Act, or associated explanatory material, should make it clear that a contextual evaluation (continues to be, and is) required in clarifying if information is "personal information";

(cont'd)

DEFINITION OF PERSONAL INFORMATION

(Continued)

- that if AGD includes a non-exhaustive list of technical data that may be captured by the definition of personal information that it be included in the explanatory memorandum/ guidance, rather than in the legislation itself.
- consider "Collection" might reasonably include the act or practice of generating or inferring information.
- that the standard of 'anonymised' is too high and there should not be a requirement for APP entities to irreversibly anonymise information to meet the threshold of "extremely remote or hypothetical";
- if "anonymisation" is to replace "de-identified" as proposed in the Discussion Paper, it needs to be clear that the standard remains 'functional' anonymisation where individuals are not identifiable by any means reasonably likely to be used.

4. Small Business Exemption

The OAIC stated in its response to the Issues Paper[17] that "Personal and sensitive information held by small business is not immune to the substantial risks that exist in the digital environment". It also stated[18] that it considered that the small business exemption was no longer appropriate in light of the privacy risks posed by entities of all sizes and the regulatory uncertainty created by the application of the 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. Many SMEs are willing to be held to the same standards as to fair and responsible handling of personal information as currently apply to APP entities. The principal issue for many SMEs is not as to 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.

[17] Office of the Australian Information Commission submission in response to the Privacy Act Review Issues Paper 2020, page 58
18 ibid

For the reasons outlined in our submission in response to the Issues Paper[19] ADMA continues to advocate that the removal of the small business exemption makes sense in order to help get Australia one step closer to an 'adequacy' decision from the European Commission (and New Zealand). Australian businesses of all sizes will benefit from improved cross border data flows.

However, inclusion of SMEs in the data privacy statute should be done in a way that recognises their more limited capabilities. 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.[20]

SMALL BUSINESS EXEMPTION

ADMA RECOMMENDATION:

- 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 help aid small businesses with awareness of and preparation for compliance with the Privacy Act.

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

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

ADMA
Intelligent Marketing

Part 2: Protections

8. Notice of collection of personal information

9. Consent to collection, use and disclosure of personal information

Summary of Proposals 8.1-8.4

- *Introduce an express requirement in APP 5 that privacy notices must be clear, current and understandable.*
- *Clarify what should be included in APP 5 notices and when they must be provided*
- *Consider Standardised privacy notices in the development of an APP code*

Summary of Proposals 9.1 and 9.2

- *Consent to be defined in the Act as being voluntary, informed, current, specific and an unambiguous indication through clear action*
- *Consider Standardised Consents in the development of an APP Code*

Privacy statutes enacted around the world over the last few decades have their data protection foundations set on a notice and consent framework. Their purpose is to ensure that individuals have knowledge of and choice and control over how information about them is handled by organisations. Implementation of obligations is through privacy policies (transparency – APP 1.3), privacy notices at time of collection (APP 5) and requests for consent (when collecting sensitive information and handling personal information beyond the primary purpose of collection – APP 3.3 and APP 6.1).

PRIVACY SELF MANAGEMENT AND TRANSPARENCY

Privacy self-management empowers individuals to make choices and exercise control around their personal information. It addresses power imbalances and information disproportions between individuals and APP entities. Transparency and notice requirements underpin the exercise of individual choice and control and hold the entity itself accountable. Transparency allows an individual to choose whether or not to exercise control in how they deal with an APP entity or whether they deal with that business at all. Transparency obligations also assist regulators, privacy and advocacy and consumer organisations to hold entities to account.

Privacy self-management also relies on entities making information about their personal information handling practices accessible and understandable. It is an opportunity for the business to build trust with those that interact and engage with it. 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 businesses data handling practices.

INFORMATION OVERLOAD, CHOICE AND NOTICE FATIGUE

Many of the submissions to the Issues Paper stage of this Privacy Review highlighted how in today's on-demand, instantaneous, information and content ubiquitous world, individuals are already overwhelmed (and fatigued) by a plethora of information. Putting the onus on a consumer to read, digest and evaluate even more information in the way of privacy policies and notices is not necessarily achieving the outcome intended. Given that individuals also engage with a number of various organisations throughout each day, the sheer volume of material they are asked to read would be a contributing factor to the findings in the *OAIC Australian Community Attitudes to Privacy Survey 2020*[21] which confirmed that while the majority of Australians believe privacy of their information to be important, only a third read privacy policies and just 20% read and understand them.

However, a person's level of interest in, or their understanding of, their legitimate interests and right in and to protection of personal information relating to them should not determine the level of protection to which they are entitled.

In addition to this, schooling, work and socialising is increasingly taking place online, and where offline alternatives are not/less of an option, individuals have little choice whether they participate. This generally means that they have to accept the information handling terms offered by the platforms or services they use. Smart devices bring yet another kind of challenge. Shared smart home/office devices can impact a broader set of people than the individual who is given notice and provided their consent. Proliferation of choice, while ostensibly a positive for consumers, has also led to an increase in frustration and confusion. Choice becomes meaningless and even detrimental if it is not structured in a way that is clear and easy for consumers to navigate and act in accordance with their preferences.

These are just some of the challenges that need to be taken into consideration when looking at how individuals can have greater confidence that they will be treated fairly no matter what they choose. ADMA also suggests that in considering the concept of consent in this Review, thought needs to be given to how best to manage the need for separate consent for the critical information required to carry out functions of a business (eg. opting out of providing your name, email, and phone number for a loyalty program renders the program useless, but you should be able to opt out of sharing gender).

ADMA agrees that the Privacy Act should continue to focus upon ready availability and comprehensibility of privacy disclosures and not increase notice or consent fatigue and to that end supports proposal 8.1 of an introduction of an express requirement in APP5 that privacy notices must be clear, current and understandable.

[21] OAIC Australian Community Attitudes to Privacy Survey,

LIMITED NOTICE REQUIREMENTS

As to Proposal 8.2 ADMA agrees an APP 5 notice should be limited to the core components outlined in the Discussion Paper[22] but this outline should be extended to include a requirement to *only state purposes to the extent that a purpose is unusual* – that is, not reasonably expected as normal or a customary incident or aspect of provision of a particular product or service.

An 'unusual' purpose is when the provision of information to the individual , (by way of a notice) would have caused the individual to pause and re-consider their provision of data, participation or continuing engagement with a service. This includes where[23]:

- the individual may not be aware that the APP entity has collected the personal information, then the APP should make known that the entity has collected personal information and the circumstances of that collection;
- whether the APP entity is likely to disclose the personal information to overseas recipients;
- the right to withdraw consent where consent has been required for the personal information handling;
- any purposes the information handling will be collected , used or disclosed where the individual is likely to find concerning, including where it will be collected, used or disclosed for a restricted practice.

The above must be provided in a manner that is succinct and appropriate, informing but not over-complicating the overall notice. All other purposes can be addressed in the transparency materials (App1.3 - privacy policy etc). This is adequate given the ease with which individuals can (through hyperlinking) move between privacy policies online, privacy collection notices and other explanatory and background materials made available online and in privacy centres. Overextending transparency also decreases the value of transparency. To require too much information upfront will absolutely increase notice fatigue and be counter-productive. It will lead to overwhelming the individual or allowing an entity to 'bury' a notice about an activity that ought to have been given prominence.

KEEPING NOTICE MEANINGFUL

Proposal 8.4 recommends strengthening the requirement for when an APP 5 collection notice is required. ADMA believes that this would impose an unreasonable burden on APP entities.

APP 5.1 currently requires that *an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure*

[22] AGD Privacy Act Review Discussion Paper, October 2021, page 70
[23] OAIC submission to the Privacy Act Review Discussion Paper, October 2021, page 69

the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection, or as soon as practicable afterwards.

ADMA believes the current wording of APP 5.1 is suitable as is. APP 5.1 creates a flexible requirement that can appropriately adapt to meet the breadth of circumstances in which information may be collected. The Discussion Paper states that *the intention of proposal 8.4 is to be more prescriptive about when notice is required so as to reduce APP entities determining at their own discretion whether to provide notice and to increase notification where information is collected indirectly*[24].

ADMA believes that proposal 8.4 would have the negative effect of requiring notice to be provided in circumstances where it may not be needed or may be harmful. As stated previously in this submission, a spill on effect of increased notification would be increased notification fatigue, which will have a detrimental effect of privacy self-management. It is instead better to ensure that notice remains meaningful.

If the overriding sentiment is that proposal 8.4 needs to be adopted, then ADMA recommends that it be stated in accompanying Guideline notes or Explanatory Materials instead so as to mitigate the potential of moving towards over-notifying individuals.

WHAT CONSTITUTES CONSENT

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

To the extent that consent is required, ADMA supports the introduction of further clarification that consent must be voluntary, informed, *reasonably* current, *reasonably* specific and unambiguous.

With regard to the wording 'through clear action' ADMA would like the Government to consider the following in its Review.

> *The current definition of consent makes clear that consent can be express or implied. Express consent is given explicitly, either orally or in writing. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity*[25].

The ability for entities to rely on implied consent is valuable (to both the individual and the APP entity) in a number of appropriate contexts. ADMA supports 'clear action' where consent is unambiguously indicated through clear action such as clicking through to use a service – provided that in each case it is demonstrable that clear action by the affected individual followed

[24] AGD Privacy Act Review Discussion Paper, October 2021, page 72-73
[25] OAIC, 'Chapter B: Key concepts', Australian Privacy Principles guidelines, oaic.gov.au, 22 July 2019,

reasonably prominent display of relevant information about the acts and practices related to which the consent is sought (ie. reasonably informed) and through the relevant clear action obtained.

ADMA does not support any reform that includes (in the legislation itself or in any explanatory materials) that consent should require specific (affirmative) action to signify express consent.

ADMA also cautions moving towards a privacy regime that expands the requirements of consent unnecessarily, as this is more likely to increase burdens upon consumers and increase 'consent fatigue' rather than empower consumers as is the intent of Privacy self-management. ADMA submits that consent requirements should remain focussed upon the collection and handling of sensitive personal information and continue to recognise that fully informed consent need not require an affirmative act by an affected individual.

That said, ADMA believes that the OAIC Guidelines should have a guide as to what is not considered "clear action", including the following from the CCPA's clarification to the definition of consent[26]:

"acceptance of a general or broad terms of use", "hovering over, muting, pausing or closing a given piece of content" and/or agreement obtained through use of dark patterns" do not constitute consent"

STANDARDISATION OF PRIVACY NOTICES AND CONSENTS

Proposal 8.3 recommends standardising privacy notices and Proposal 9.2 recommends standardising consents.

While ADMA can see that there are some benefits in standardisation assisting individuals in becoming familiar with the various components of privacy notices and wording for consent, and may very well allow for a level of comparison between different services, ADMA is more concerned about the context where mandating standardisation can risk introducing regulated rigidities that impede better communication, more targeted, directed and context specific disclosure and continuous improvements. This is especially so in the data-driven marketing and advertising industry where responsible marketers often look to their competitors to learn from, improve on and/or differentiate themselves as to how they roll out and/or promote their own transparency measures. This is particularly important to data-driven marketers who see such as opportunities to build consumer trust. Too much standardisation could also lead to having the opposite effect of consumers making assumptions about disclosures rather than reading what the APP entity is disclosing.

The Discussion Paper also outlines that, it may be impractical to develop standardised forms of consent across all sectors, due to the wide range of contexts in which the Privacy Act applies.

[26] The California Consumer Privacy Act – as amended through Assembly Bill 694 on privacy and consumer protection. The amended Act took effect on 1 January

In addition to this, ADMA also recognises that statute-specific, regulated rigidities as to the form and content of privacy disclosures will create significant costs for APP entities that provide products and services across national borders, where these entities are required to include additions to address diverse national requirements. These such entities should not be so regulated as to not be able to provide the required information to individuals in the clearest possible way (as per Proposal 8.1).

It is different if standardisation is offered *as a guidance* to assist entities with their drafting of consents and privacy policies as this may assist those APP entities who would find a point of reference helpful. ADMA considers that rather than including within an APP Code, that instead perhaps the OAIC Guidelines offer guidance on sector-specific standardisation as a more appropriate way of assisting individuals and APP entities with their understanding and decision-making in relation to both consent and what should be included in respective privacy policies.

NOTICE & CONSENT

ADMA RECOMMENDATION:

- ADMA strongly supports Proposal 8.1 that an express requirement is introduced in APP 5 that notices must be clear, current and understandable.
- ADMA recommends that in relation to Proposal 8.2, that APP 5 notices be limited to the matters listed in the Discussion Paper[1] and purposes *"to the extent that a purpose is unusual or unexpected"*. Any inclusion of such notice must be done succinctly and as appropriate to inform but not over-complicate the overall notice.
- ADMA believes that the implementation of Proposal 8.4 would impose an unreasonable burden on APP entities and that the current wording of APP 5.1 is suitable as is.

  However, if the overriding sentiment is that proposal 8.4 needs to be adopted, then ADMA recommends that it be stated in accompanying Guideline notes or Explanatory Materials instead so as to mitigate the potential of a shift towards over-notifying individuals.

- To the extent that consent is required, ADMA supports the definition of Consent outlined in Proposal 9.1, with the addition of the qualifier (as underlined for ease of reference below);

  "consent must be voluntary, informed, reasonably current, reasonably specific and unambiguous."

  to the extent that it instead reads that: being voluntary, informed, reasonably current, reasonably specific and an unambiguous *indication through clear action*.

- ADMA does not support an amendment that would in any way look to include that 'clear action' require specific affirmative action.
- ADMA does not support Proposal 8.3 (standardisation of privacy policies) or Proposal 9.2 (standardisation of consents), believing that the burden on APP entities would be unreasonable and likely be a detriment for the innovative improvement of privacy self-management that occurs organically in a competitive society.

ADMA
Intelligent Marketing

10 – Additional protections for collection, use and disclosure

Summary of Proposals 10.1 – 10.4

- *A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances*
- *Create a list of legislated factors relevant to whether a collection, use or disclosure of personal information is 'fair and reasonable in the circumstances'*
- *Include an additional requirement in APP 3.6 to the effect that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3*
- *Define allowable 'primary' and 'secondary' purpose for use and disclosure at APP 6*

For the most part to date, transparency and privacy self-management requirements in the Privacy Act have been reasonably sufficient to enable individuals to be informed about their data and take the necessary steps to protect themselves. The digital economy has, however, brought about a range of different technologies on/through which personal information is shared as well as a rapid and substantial increase in the amount of personal information collected, used and disclosed. This has impacted the effectiveness of the data privacy regimes that rely heavily on privacy self-management, notice and consent. Individuals are continuously receiving updates on how their personal information is being handled, as businesses update the ways in which they need to use such information and then notify accordingly. The need to share personal information for the purposes of processing and campaign management is also increasing and changing constantly. It has become unrealistic to assume that individuals are taking the time to consider and understand every update on privacy that they are notified of and to then take the steps to protect themselves from privacy harms.

AN ASSUMPTION OF SAFETY

As stated by the Joint Committee on Human Rights of the UK Parliament in its Inquiry Report on the Right to Privacy (Article 8) and the Digital Revolution[27]:

> The system should be designed so that we are protected without requiring us to understand and to police whether our freedoms are being protected….. "*If you enter a building, you do not sign away your rights to enter it safely. You do not sign a form with 14,000 pages that tells you how the building was built and that says you have to accept the risk. You rely on the fact that the architect, the engineer and the builder will be subject to regulation, and that there will be insurance and public liability requirements on the building because it is open to the public, and you will feel that you can then walk into that building safely.*

[27] Report of the UK House of Commons and House of Lords, Joint Committee on Human Rights, "The Right to Privacy (Article 8) and the Digital Revolution", HC 122, HL Paper 14, published on 3 November 2019 – page 12

> *The companies that build data systems describe themselves as architects and engineers, so it is unfair on an individual to expect them to take responsibility for any risks, and there are serious risks of harm associated with using web-based services."*

Individuals should be able to take a certain level of data privacy safety for granted. 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.

Introducing a threshold test that holds regulated entities to account, can improve the behaviours of these entities and help to build a more trustworthy digital economy and have the added effect of avoiding heavier reliance on consent. As privacy regimes around the globe improve their privacy and data laws, and courts internationally are seen to hold businesses to a higher level of accountability, the community at large has come to expect more from organisations than that which is currently prescribed by the Australian Privacy Act.

A current weakness in the Australian Privacy Act is that where a collection, use or disclosure of personal information is clearly and broadly harmful, the Privacy Act should prohibit it without falling to the user to identify and avoid or mitigate that harm.

THE PROPOSAL TO INTRODUCE AN OVERARCHING THRESHOLD TEST

An overarching threshold test should rule out the most exploitative data practices and provide a basis for trust, by shifting responsibility for avoiding harms towards APP entities that effect those harms. A well designed requirement would have the effect of lowering the level of vigilance required to protect against everyday privacy harms and improve digital trust, while also allowing businesses freedom to operate within appropriate bounds.

ADMA does **not** believe that the addition of the "fair and *reasonable*" test as outlined in proposal 10.1, is appropriate, nor would it achieve the goals of building trust around the privacy protection regulatory framework. This is because such a test has the potential of introducing substantial uncertainty into data privacy governance, compliance and data risk assurance processes of regulated entities.

'Reasonableness' as an over-arching positive legal requirement is highly subjective – which is one of the reasons why it has not been adopted into Australian consumer protection statutes to date.

The Privacy Act already requires "fairness" as to the means of collection of personal information (APP 3.5[28]) which is an appropriate and sufficient control as to excessive or intrusive data

28 Under the current test at APP 3.5, whether a means of collecting information is fair will depend on the circumstances but includes collections that do not involve intimidation or deception and are not unreasonably intrusive. For more information, see OAIC, Chapter 3: APP 3 – Collection of solicited personal information Australian Privacy Principles guidelines, oaic.gov.au, 22 July 2019,

collection practices". "Fair" puts the individual at the centre of the privacy framework and this ensures that the community at large is protected from privacy harms. Considering what is fair to the individual also helps entities, that are trying to do the right thing, keep a check on the way they handle personal information responsibly with the knowledge that they can go about *their functions and activities to the extent that those functions and activities are consistent with benefit to Australian society* (as discussed to be the Object of the Act as put forward in Proposal 1.1). If something is deemed to be unfair, then it is for all intents and purposes a 'no-go'.

Raising the general standard of personal information handling across the economy requires that APP entities are more accountable for their information handling practices by requiring them to meet a standard that is appropriate and fair. In Canada[29] 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 and 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". Another approach to consider would be the EU GDPR, where Chapter 2 outlines the factors to be considered in decision-making.[30] Australia could follow this approach by streamlining and strengthening existing requirements of the Act.

CLEAR UNAMBIGUOUS GUIDANCE IF THE THRESHOLD TEST IS INTRODUCED

While ADMA supports the intention behind the fairness test, it does not support Proposal 10.1 in the form recommended ("fair and reasonable" test) as there are limitations including "reasonableness" as the benchmark.

If however, if the recommended proposal 10.1 was to be adopted into legislature then for it to survive the test of time there would need to be very clear additional guidance provided on how to meet the test and, equally, what would *not* meet the test. The absence of any such guidance could lead to ambiguity and complexity. The guidelines to the threshold test could list protected categories of data and ensure that the use of such data must align to the legitimate interest of the entity and the expectations of the reasonable consumer. If it does not align then is ruled out.

The challenge will be to consider the application of the test and provide guidance that is neither too restrictive or too broad, that keeps the individuals privacy protection at the core and doesn't negatively impact competition and the ability for APP entities to innovate. Getting this balance wrong will inevitably lead to privacy harms.

[29] 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

[30] Chapter 2, European Union, General Data Protection Regulation

If a threshold test is to be included in the Act, careful attention will also need to be given to how the fairness test is incorporated into APPs 3 and 6. It will need to be clear to all readers of the legislation that this test (as included in the regulation and explained in the Guiding material) is a threshold test, so if a personal information handling practice fails to meet this fairness test, then it will be prohibited, regardless of the lawful ground that could otherwise be relied upon.

ADMA recommends the Government further consider whether there are less broadly subjective alternate options (to "reasonable") for a threshold test, perhaps looking to other data privacy regimes, comparable legislation locally and engaging a cross sector of industry to discuss whether, if "reasonable" has no alternative – what qualifiers would need to be considered so as to achieve the purpose intended.

The Act already requires fairness as to the means of collection of personal information (per APP 3.5) so a threshold test would need to provide *further* certainty if it is to be included.

PRIMARY AND SECONDARY PURPOSE FOR USE AND DISCLOSURE

Proposal 10.4 recommends the definition of primary purpose and secondary purpose for use and disclosure in APP 6

ADMA agrees with the OAIC's statement[31] that

> *Purpose specification is an essential principle that underpins privacy laws globally. The purpose specification principle, together with the use limitation principle, requires that individuals be notified of the purposes for which their personal information was collected and limits the uses of information to those purposes unless an exception applies. These principles promote data minimisation by ensuring that information is only collected and held where there is a valid purpose for its use.*

However , the ACCC in its DPI Final Report, highlighted the limitation in this framework which allowed certain digital platforms to set out vague or overly broad[32] primary purposes in their privacy policies.

ADMA therefore supports the need for clarity and certainty in this area. The definition of primary purpose in proposal 10.4 aims to provide additional certainty and encourage APP entities to classify and include a greater range of uses and disclosures as primary purposes. ADMA is concerned that this approach would circle back to further increasing complexity and length of privacy notices and disclosures. This could ultimately lead to the same outcome the DPI Final Report highlighted, but instead of vague or overly broad, it could be overwhelming and there is

[31] OAIC submission to the Privacy Act Review Discussion Paper, October 2021, page 91

[32] ACCC, *Digital Platforms Inquiry – Final Report*, ACCC, July 2019, accessed on 24 November 2021, p 438.

the risk that entities with a motivation to do, so could bury within a long list an intended purpose that may be of concern to the individual to which the information relates to.

This proposal may also incentivise an overly legalistic approach to defining primary purposes in an APP 5 notice. ADMA does not support proposal 10.4 with regards to primary purpose.

With regard to the recommendation on the definition of secondary purpose ADMA suggests that consideration be given to appropriately frame the exceptions for specified legitimate interests, legitimate uses or compatible data practices rather than trying to limit a permitted "secondary purpose" to an act or practice that is "reasonably necessary to support the primary purpose". A valid (and legitimate) secondary purpose could be to use customer data to do research to improve a product or service, which would benefit consumers but would not be considered to be "reasonably necessary to support the primary purpose".

If the secondary purpose were to be defined as proposed in the Discussion paper, it would inevitably mean that in order to cover all possible secondary purposes, the entity would expand their stated primary purpose leading yet again to the increased complexity and length of privacy notice as disclosures.

Defining "secondary purpose" as, *"a purpose that is directly related to, and reasonably necessary to support the primary purpose"*, could also have the effect of narrowing the scope of the data being used for socially beneficial uses which could ultimately impede its use in innovation required to improve quality of life and other developments. An option that the Government could consider is the development of a third tier (tertiary purpose) to clearly identify when personal information may be used for socially beneficial uses such as public interest research, particularly if information is aggregated and de-identified. This can create a clear distinction between data that is used for a specific purpose that may relate to the experience of an individual or group of consumers and when data is part of a broader study. There may need to be an additional requirement as to the level or category of disclosure permitted, depending on the kind of information encapsulated in this tier.

ADDITIONAL PROTECTIONS FOR COLLECTION USE & DISCLOSURE

ADMA RECOMMENDATIONS:

- **ADMA supports the *intention* behind an overarching threshold test which for individuals present a stronger baseline protection against real and substantial concerns.**
- **ADMA does not support Proposal 10.1 in the form recommended ("fair and reasonable" test) as there are limitations including "reasonableness" as the benchmark.**
- **ADMA recommends the Government further consider alternate options for a threshold test, perhaps looking to other data privacy regimes, comparable legislation locally and engaging a cross sector of industry to discuss whether, if "reasonable" has no alternative – what qualifiers would need to be considered so as to achieve the purpose intended.**

(cont'd)

ADDITIONAL PROTECTIONS FOR COLLECTION USE & DISCLOSURE

(Continued)

- ADMA notes that the Act already requires fairness as to the means of collection of personal information (per APP 3.5) so a threshold test would need to provide further certainty if it is to be included.
- ADMA supports the intention behind proposal 10.4 however ADMA is concerned the definitions as provided in proposal 10.4 would in practice create other problems as to the complexity and length of such APP 5 notices.

14 – Right to object and portability

Proposal 14
Introduce a requirement that an individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information. On receiving notice of an objection, an entity must take reasonable steps to stop collecting, using or disclosing the individual's personal information and must inform the individual of the consequences of the objection.

Proposal 14 is to introduce a qualified right to opt out of the collection use and disclosure of one's personal information. This proposal ought to be read alongside Proposal 16 (addressed below in this submission) – which recommends an absolute right to opt out of direct marketing.

ADMA believes that the recommendation in Proposal 14.1 is far too broadly stated to be considered reasonable or even practical.

A right to object should relate to data collection, use and disclosure that is not required to enable the basic functioning of an online service. In any event, where uses and disclosures are a reasonable incident of provision of a service, an affected individual may elect to not acquire or otherwise use the product or service.

With regards to ***withdrawing consent***, Proposal 14 deals only with situations in which consent is being withdrawn, which means it is restricted to circumstances where "with consent" was the lawful ground for authorisation to collect sensitive information under APP 3 and/or to use or disclose personal information under APP 6. Given that consent is required to be freely given in the first place, then it must already, under the law be able to be withdrawn as easily as it was given. Essentially Proposal 14 is just recommending the formalisation in statue that an organisation must have the mechanism to withdraw consent (where consent is being relied on in the first place).

ADMA is unclear as to the practical difference between the existing and recommended approach.

To the extent that the legislature considers it appropriate to provide affected individuals a right to elect to opt out then ADMA recommends that the right to "object" should only relate to data collection, use and disclosure that is not required to enable the basic functioning of an online service and is consistent with other regulatory obligations such as Know Your Customer (KYC).

THE RIGHT TO OBJECT

ADMA RECOMMENDATIONS:

- ADMA does not support the "Right to Object" as recommended in Proposal 14, believing it to be too broad and therefore not practical.
- To the extent that the legislature considers it appropriate to provide affected individuals a right to elect to opt out then ADMA recommends that the right to "*object*" should only relate to data collection, use and disclosure that is not required to enable the basic functioning of an online service and is consistent with other regulatory obligations such as Know Your Customer (KYC).

16 – Direct Marketing, Targeted advertising and profiling

Summary of Proposal 16:

- *To repeal APP 7*
- *To extend the "right to object" (Proposal 14) to be an unqualified right to opt out of collection, use or disclosure for direct marketing*
- *To require notification to individuals of their right to object*
- *To require that any "use or disclosure of personal information for the purpose of influencing an individuals behaviour or decisions must be a primary purpose notified to the individual when their personal information is collected"*
- *To require additional information about marketing be included in an entity's Privacy Policy*

ADMA supports amendments to the way data privacy regulation addresses direct marketing. ADMA supports such amendments so long as they are focused on addressing the real privacy harms that come about from the actions of bad actors who look to exploit the weaknesses within Act as it currently stands, as well as those organisations that are careless, ignorant, uncaring and negligent towards their privacy obligations. The actions of these cohorts undermine the collective efforts of responsible marketers who are focussed on harnessing data in a responsible and innovative way to better achieve their business and marketing goals and give the end consumer a trusted valuable user experience.

ADMA considers Proposal 16 and suggests that further adjustments need to be made.

NOT ALL DIRECT MARKETING HAS A HIGH PRIVACY IMPACT

First, we note upfront that not all forms of direct marketing have a high privacy impact, even when delivered at scale. For example, an email newsletter delivered to the first party subscribers of a retailer poses very low privacy risk if there is no personalisation of messaging or pricing. Therefore, we request that the review and/or introduction of regulation in this space must appropriately distinguish between the more intrusive and covert tracking and profiling activities (collection of data across unrelated websites, apps, services and devices) which power online behavioural advertising at one end of the scale, and a business sending an email to its existing customer base at the other.

DIRECT MARKETING AND PRE-EXISTING RELATIONSHIPS

As stated in our response to the Issues Paper, ADMA submits that the delivery of direct marketing to an individual with whom an organisation has a direct pre-existing relationship (in whatever form that may have initiated) should remain lawful, on an opt-out basis. This includes (without limitation) a past customer, someone who has made an enquiry of the APP entity, entered a competition where the APP entity was the Promoter, signed up to join a database or taken up an offer of any kind from the APP entity.

APPs that engage in direct marketing may have an operational reliance on being able to provide customer data to a third-party contractor, such as a mailing house, for the purpose of using that data to deliver communications reasonably expected by the recipient. Therefore an amendment to the current regulation must be done without blocking out the ability of an APP entity to continue to do this responsibly.

Marketing by third parties, or the use of secondary party or third-party customer data via online behavioural advertising, should be able to be done with the individual's consent (as obtained in a manner that is voluntary, informed, reasonably current, reasonably specific and unambiguous, as suggested above in Proposal 9.1).

THE DEFINITION OF 'DIRECT MARKETING'

Direct marketing is a term that has historically been used with some clarity; however, in a digital economy that clarity is becoming clouded. ADMA questions whether the term direct marketing is still the most suitable one to correctly reflect the range of activity that the Act aims to regulate. "Direct marketing" is not defined in the Privacy Act. However, the Australian Privacy Commissioner in the Australian Privacy Principles guidelines (February 2014) expressed the view that *"direct marketing involves the use and/or disclosure of personal information to communicate directly with an individual to promote goods and services. A direct marketer may communicate with an individual through a variety of channels, including telephone, SMS, mail, email and online advertising"*.

If the proposal to Repeal APP 7 is confirmed, there might be an opportunity to either re-define the phrase (term) or replace it with a different descriptor so as to avoid the historical application which could create confusion. Whether the definition of direct marketing changes or remains as stated by the Commissioner, ADMA suggests that 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 could have some particular relevance if an individual requests to withdraw consent or uses their right to object to the collection, use and disclosure of their personal information.

DIRECT MARKETING AND AN UNQUALIFIED RIGHT TO OBJECT

Proposal 16.1 recommends that the right to object discussed in Proposal 14 would include an *unqualified* right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing.

ADMA notes Proposal 16.1 is different to proposal 14, in that Proposal 14 has a general right to object and Proposal 16.1 puts forward an *unqualified* right, where 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 that 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 16.1.

If APP 7 is repealed (and the reference to it in APP 6 is also removed) then "direct marketing" as it is defined by the Privacy Commissioner in the OAIC Guidance[33] falls under APP 6 "use and disclosure of personal information" requirements. Under APP 6 *"all use and disclosure activities, (whether for marketing or other purposes), must be able to be justified on one or more lawful grounds, such as primary purpose, 'directly related secondary purpose' or 'with consent'."*

As discussed previously in this submission under proposal 14:

> In relation to "with consent" - given that consent is required to be freely given in the first place, then it must already under the law be able to be withdrawn as easily as it was given.

[33] Australian Privacy Commissioner in the Australian Privacy Principles guidelines (February 2014) expressed the view that "direct marketing involves the use and/or disclosure of personal information to communicate directly with an individual to promote goods and services. A direct marketer may communicate with an individual through a variety of channels, including telephone, SMS, mail, email and online advertising."

ADMA believes that there is no need to include, in addition to Proposal 14, an unqualified right to object related to direct marketing usage of personal information" as the law would already, in practice, cover what it is hoping to achieve.

To the extent that the legislature considers that it is appropriate for the Act to afford affected individuals a right to opt-out of collection, or from particular uses or disclosures of personal information about them , then that right should:

- be created through and specified in legislature settings and not through exercise of discretion by the regulator;
- relate specifically to and be separately exercisable in relation to uses and disclosure of personal information for the purpose of targeted online advertising and other forms of direct marketing based upon differentiation between individuals;
- to the extent mandated for, or voluntarily offered in relation to, any context other than targeted online advertising and other forms of direct marketing based upon differentiation between individuals, be separated from the opt out for targeting and direct marketing and to the end it is required for provision of a product or service (ie. what is considered under the SPAM Act as service statements);
- not include audience segmentation-based marketing where the factors (inferred interests or preferences or other characteristics) used to define the audience segment used for delivery of content was not created through the use of personally identifying information;
- there is no disclosure of personal identifying information; and
- relevant factors are not added to profile information about an identifiable individual.

DIRECT MARKETING AND OTHER REGULATIONS

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

The requirement to include a functional unsubscribe link or similar opt-out mechanism would replicate the practice already regulating direct marketing (via APP 7 and the SPAM Act), but would broaden it to other forms of direct marketing. Consideration of whether this is practical or not would depend on what is included in the definition of direct marketing.

ADMA's submission in response to the Issues Paper highlighted the Canadian approach of allowing most forms of online behavioural advertising so long as individuals can easily opt out. The effect is to prohibit practices which do not support user control (such as zombie cookies).

DEFINING DIRECT MARKETING AS A PRIMARY PURPOSE

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

ADMA does not support this proposal as it will likely obliterate all forms of marketing (direct and indirect, harmful or not). At the very least it would be an impractical statement from almost all APP entities. While marketing and targeting to influence behaviour or a purchasing decision is likely a common purpose across all commercial businesses, and would be expected by consumers, it would be a stretch to characterise it to be a "primary purpose" of most organisations. A more accurate description of marketing would instead be - a "directly related secondary purpose" of the service they provide. This understanding would also be shared an organisations clients and the individuals that engage with them.

DIRECT MARKETING AND THE CCPA

With regard to direct marketing and the Privacy Act, ADMA suggests considering the way the CCPA addresses the protection against the more concerning privacy harms.

The CCPA specifically includes marketing activities such as counting ad impressions and verifying ad quality as legitimate business uses for personal information. This is an important carve out, as it protects the integrity of digital systems (both advertising and non-advertising based) and is required to prevent overall societal harm, including fake website traffic and fraudulent comments. The collection of data to protect the integrity of online systems should not be considered a privacy harm or risk, provided data used for this purpose is not used for a secondary marketing purpose. Likewise, mobile phone numbers are increasingly required for security (in multi-factor authentication) but provision of this data for security should not automatically be considered consent to use this number for other purposes.

CCPA also provides individuals with the right to opt-out or say no to the sale of their personal information.

In addition, the CCPA includes a right of consumers not to be discriminated against, even if they exercise their data privacy rights. This reduces the following types of actions that would possibly be seen as discriminatory and likely be of most concern:

- denying goods or services to a consumer;
- charging different prices or rates for goods or services, including through the use of discounts or imposing penalties;
- providing a different level or quality of goods or services to the consumer;
- suggesting that the consumer would receive a different price or rate for goods or services or a different level or quality of goods or services.

ADMA
Intelligent Marketing

DIRECT MARKETING, TARGETED ADVERTISING & PROFILING

ADMA RECOMMENDATIONS:

- ADMA is not opposed to the proposal that APP 7 is repealed and believes that direct marketing could be managed suitably as all other personal information is under APP 6.
- ADMA does not support Proposal 16.1 recommending inclusion of "*an unqualified right to object related to direct marketing usage of personal information*" as the law would already, in practice, cover what it is hoping to achieve.
- To the extent that the legislature considers that it is appropriate for the Act to afford affected individuals a right of election to opt-out of collection, or from particular uses or disclosures of personal information about them, then that right should:

    - be created through and specified in legislature settings and not through exercise of discretion by the regulator;
    - relate specifically to and be separately exercisable in relation to uses and disclosure of personal information for the purpose of targeted online advertising and other forms of direct marketing based upon differentiation between individuals,
    - only be available in respect of personal information that is being processed on the ground of consent;
    - to the extent mandated for, or voluntarily offered in relation to, any context other than targeted online advertising and other forms of direct marketing based upon differentiation between individuals, be separated from the opt-out for targeting and direct marketing and to the end it is required for provision of a product or service (ie. what is considered under the SPAM Act as service statements);
    - not include audience segmentation-based marketing where the factors (inferred interests or preferences or other characteristics) used to define the audience segment used for delivery of content was not created through the use of personally identifying information;
    - there is no disclosure of personal identifying information and relevant factors are not added to profile information about an identifiable individual.

- ADMA believes there might be an opportunity to either redefine the phrase "direct marketing" or replace it with a different descriptor in order to clarify the range of activities expected to be undertaken by a modern organisation. Either way, ADMA recommends that there is room for widespread education for APP entities and the community at large to better understand the phrase.
- ADMA does not support Proposal 16.2 in its recommendation that "use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions must be a primary purpose notified to the individual when their personal information is collected".
- ADMA recommends that in dealing with direct marketing in this Review, that the Government look to the way in which the Canadian privacy laws and the CCPA consider the more serious risks to privacy protection.

21. Controllers and processors of personal information

The Privacy Act makes no distinction between entities that control and those that process personal data. Any handling by APP entities of personal data, whether collecting, using, disclosing, holding or otherwise processing it, either independently or on the instructions of another organisation, is potentially subject to regulation under the Privacy Act.

Introducing the controller/processor distinction into the Privacy Act may help to clarify application of the APPs and also improve organisational accountability. Introduction of controller/processor will ensure that responsibility between the parties is clearly allocated based on the actual control over the handling of personal information. The distinction will also minimise duplication of effort for businesses (complying with obligations) and individuals (dealing with duplication in notice and requests for consent).

A data controller can process collected data using its own processes or may have to work with a third-party or an external service. Even in this situation, the data controller will not relinquish control of the data to the third-party service. The data controller will remain in control by specifying how the data is going to be used and processed by that external service. This is where it is important to have appropriate technical and operational documents, processes and controls around the handling of any personal information that an APP entity holds, even if the entity is a processor.

The Discussion Paper mentions the potential gaps that would exist if the small business exemption is maintained. The Discussion Paper suggests that these gaps could be resolved if the controller/processor distinction only applied where both parties are APP entities.

However, given the likelihood that there are many potential data processors that may exist only to serve and support small businesses, this could potentially present risk exposure to privacy harms. This is especially possible if a bad actor were to concentrate on targeting this particular cohort. To avoid this risk exposure, perhaps there would be instances where a data processor will need to be subject to organisational accountability obligations under APP 1 and security requirements of APP 11 in order to mitigate this risk.

The Discussion Paper outlines that introduction of the controller/processor distinction would also align Australian's privacy regime with other international data privacy regimes such as GDPR, CBPR and the domestic privacy laws of New Zealand, Brazil, Japan, Hong Kong and Singapore. Canada and India are also putting forward drafts signalling their intention to move a similar way.

ADMA acknowledges that the potential benefits of introducing controller/processor needs to be weighed against the potential increase in complexity that the controller/processor

distinction may add to the data privacy framework. Nevertheless, ADMA believes that it is a worthwhile consideration in this Privacy Reform.

CONTROLLERS & PROCESSORS OF PERSONAL INFORMATION

ADMA RECOMMENDATION:

ADMA supports the Government considering the introduction of the controller/processor distinction into the Privacy Act but recognises there will need to be consideration given as to how accountability is applied in certain circumstances (ie. in relation to data processors, especially if the small business exemption remains.

22. Overseas data flow

As the digital economy develops, the amount of data and instances in which data flows across borders increases. Technological solutions, including cloud computing infrastructure, and the ease with which cross border transactions of goods and services and connections occur means that data flow is an indispensable contributing factor of almost any economic activity today.

Many entities under Australian data privacy laws already conduct operations in multiple jurisdiction, or have ambitions to.

To allow Australian businesses to remain competitive both domestically and internationally, where possible and to the extent that it doesn't call for compromise on the requirements of Australian regulatory protection of an individual's right to data privacy, Australia should strive to maximise the interoperability of data privacy regimes. This does not necessarily mean adopting other laws but instead considering how to create consistently high data privacy standards globally.

The notion of adequacy, that is the mutual recognition that the protections of a foreign data privacy regime are adequate, is the key enabler for interoperability in the absence of one common regime covering all economies across which data is processed/transferred[34]. ADMA recognises that its member-base would benefit from the Australian privacy regime moving closer towards adequacy with respect to the GDPR and New Zealand Privacy regime as many of the member-businesses have international dealings.

Also, the closer towards adequacy Australia's data privacy regime moves, the more attractive Australian innovation, business and data-based export activities will become.

For the sake of avoiding uncertainty when dealing with international partners and service providers, Australian entities presently rely on binding corporate rules or contractual clauses to

[34] Association for Data driven marketing and advertising submission in response to the Attorney-Generals Review of the Privacy Act 1988 (Cth) October 2021, page 20

insert and clarify accountability. ADMA suggests that even with reform, this method of providing clarification may be appropriate.

OVERSEAS DATA FLOW

ADMA RECOMMENDATIONS:

- ADMA supports efforts that move toward making Australia's data privacy regime closer to adequacy to the extent that any reform of regulations is what is most suitable for Australia's privacy regime.

- To support and provide clarity for APP entities that deal with global partners and the flow of data and data obligations overseas, ADMA recommends that the Privacy Act sets out a non-exhaustive, but clear, list of measures that an entity can take to demonstrate that it has taken reasonable steps, such as:
    - the discloser assesses that the recipient is bound by comparable obligations under their applicable laws;
    - the recipient is bound by corporate rules;
    - the discloser enters into contractual terms imposing data privacy (data protection) obligations on the recipient that are appropriate for the nature of the relationship between the parties and the data involved; or
    - the recipient has established systems and processes that comply to internationally recognised standards such as ISO certifications.

Conclusion

The Association of Data-driven Marketing and Advertising looks forward to continued engagement with the Attorney-General's Department, the Office of the Australian Information Commissioner and other stakeholders involved in this important review of the Privacy Act. While changes in the data privacy regime will have economy-wide application, it will directly affect the core activities of the data-driven marketing and advertising industry.

As a consequence, ADMA is keen to support all key stakeholders however it can to ensure that the review of the Privacy Act and regulatory regime is considered both through reform of the instrument itself and its application to industry. This will help ensure that Australia's data privacy framework will be fit-for-purpose and the regime will be future-proof to the extent that it can be while executing its objective and purpose effectively.

ADMA prides itself in championing excellence in responsible marketing and actively empowers its members through education, representation and advocacy of fair, transparent and responsible data-driven marketing. Any involvement to better develop this space is welcome.

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 members take their privacy compliance responsibilities very seriously and support a regime that protects the personal information of the consumers understanding that responsible marketing practices stem from a compliance with data privacy law.

ADMA is keen to support all key stakeholders, however it can to ensure that the review of the Privacy Act and regulatory regime is considered both through reform of the instrument itself and it's application to industry. This will help ensure that Australia's data privacy framework will be fit-for-purpose and the regime will be future proof to the extent that it can be while executing its objective and purpose effectively.

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.