COMMUNICATIONS
ALLIANCE LTD

Communications Alliance Submission

to the Attorney-General's Department
in response to the

Privacy Act Review Report 2022

31 March 2023

CONTENTS

Communications Alliance

Communications Alliance is the primary communications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, platform providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to be the most influential association in Australian communications, co-operatively initiating programs that promote sustainable industry development, innovation and growth, while generating positive outcomes for customers and society.

The prime mission of Communications Alliance is to create a co-operative stakeholder environment that allows the industry to take the lead on initiatives which grow the Australian communications industry, enhance the connectivity of all Australians and foster the highest standards of business behaviour.

For more details about Communications Alliance, see http://www.commsalliance.com.au.

Executive summary

Communications Alliance welcomes the opportunity to make a submission to the Attorney-General's Department (AGD) in response to the Privacy Act Review Report 2022 (Report).

We continue to support a review of the adequacy of the privacy regime and remain keen to engage with all stakeholders to ensure that improvements to privacy legislation can benefit all sectors of the economy and benefits Australia on a global stage.

Our members take privacy very seriously, and they support a privacy regime that protects the personal information of their customers, while accommodating respectful and fair collection and use of customer data.

We acknowledge that the changes brought about by the digital age require ongoing consideration and informed debate from all angles of our society and economy. Our members have invested, and will continue to invest, substantial resources in technological, process and human resource developments to ensure privacy practices remain at the highest level and keep pace with latest societal, technological and legal developments.

This review provides an opportunity for the legislature to:

- address uncertainties as to operation of the Australian *Privacy Act 1988* (Act);
- provide additional protections of the interests of individuals in data privacy, to the extent that these additional protections are appropriate and reasonably required to give effect to now commonly accepted international norms; and
- reduce friction of cross-border dealings, including for Australian businesses expanding globally, by improving alignment of the Act with leading data privacy and data protection statutes in other jurisdictions.

Reforming a data privacy statute is particularly complex. Expansion in legal principles-based requirements can readily lead to unintended consequences, particularly as a result of unforeseeable developments in utilisation of technologies and data analytics capabilities and continuing expansion in data points relating to devices and humans. Many societally beneficial applications of smart devices and smart infrastructure are dependent upon legislative and regulatory settings being appropriate to permit responsible deployment and use, while also protecting data privacy of individuals. At the same time, societies are mindful of individuals' right to control information, to the extent it personally identifies them and proportionate and practical in the circumstances.

Against this background, we highlight that particular caution should be exercised concerning the implications of the proposed revised definition of personal information and the (intended) resultant extension to metadata and technical identifiers. Similarly, further consideration ought to be given to the meaning of 'de-identification' of personal information and its practical application in relation to the definition of personal information.

It is imperative that the new legislation does not take an over-expansive approach – in an increasingly digitised age, any regime has to remain practical, and the rights assigned to the individual ought to remain proportionate to the benefits that the individual can derive from the respective information being treated as personal information, with resultant rights for the individual in relation to that information. Therefore, it is equally important to carefully develop an exceptions regime, to account for the circumstantial nature around notice, consent, collection, access, erasure etc. of personal information.

Particular care needs to be taken to ensure that the revised Act does not impede Australia deriving societal benefits from existing technologies, including those used to deliver essential products and services, as well as from the take-up of smart devices and deployment of smart infrastructure. These benefits can be achieved without compromising the need to ensure that individuals are not exposed to and suffer relevant privacy harms.

However, more work is required in relation to achieving an appropriate balance in relation to the use of technical identifiers and personalisation of services to deliver consumer benefits and preserve the right of the individual to not be unduly targeted.

Many entities regulated under Australian data privacy laws already conduct operations in multiple jurisdictions or have ambitions to do so. It is, therefore, important to align the Act with leading data privacy and data protection statutes in other jurisdictions, and to take experiences from international jurisdictions that have already implemented particular privacy-related concepts.

This includes the integration of a well-developed data processor – controller distinction which permeates the various concepts of the Act, i.e., from consent collection to a notification for an eligible data breach.

If Australia elects to chart its own course, Australian entities may be forced to incur substantial regulation-induced costs in adapting data architectures, analytics processes and data handling practices, for cross-border dealings. Australian policymakers should exercise particular caution to avoid, wherever reasonably practicable, devising regulatory measures that lead to Australia-specific, regulation-induced, costs for Australian entities in cross-border dealings.

1. Personal information, de-identification and sensitive information

Expanded definition of personal information

1.1. The Report proposes a change to the definition of personal information of the *Privacy Act 1988* (Act) by changing the word 'about' to 'relates to' (Proposal 4.1). The proposed new definition of personal information, therefore, reads [emphasis added]:

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 or opinion is recorded in a material form or not.

1.2. We note there was discussion in the Attorney-General's Department, *Privacy Act Review Discussion Paper*, October 2021 (Discussion Paper) to define the term 'reasonably identifiable', which forms part of the Act's definition of personal information. The proposed amendment to 'reasonably identifiable' would have covered circumstances in which an individual could be identified, directly or indirectly. However, the Report concludes that the inclusion of the terms 'directly or indirectly' may not solve the lack of clarity. We support this conclusion.

1.3. Instead, the Report proposes:

- *confining the definition of personal information to one where "the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance"*[1],
- *that there should be an inclusion of a "non-exhaustive list of information that may be personal information"*[2]*; and*
- *that "'Reasonably identifiable' should be supported by a non-exhaustive list of circumstances to which APP entities will be expected to have regard in their assessment."*[3]

1.4. It is critical that any amendment of the definition of personal information (to replace 'about' with 'relates to') must be carefully confined to situations where the connection between the information and the individual is not too tenuous or remote. We raised these concerns in our submission in response to the Discussion Paper, and continue to hold these views.

1.5. This is particularly important in the communications sector, where an amended definition (as proposed) could lead to the inclusion of technical identifiers and so-called metadata that were previously not included in the definition of personal information.

1.6. Consequently, whether an amended definition of personal information is practical in our sector critically depends on the appropriate inclusion of context in the definition, together with carefully crafted exceptions to individual rights, such as the right to access and explanation, and the right to erasure.

1.7. At Proposal 4.2, the Report further proposes to:

"Include a non-exhaustive list of information which may be personal information to assist APP entities to identify the types of information which could fall within the definition. Supplement this list with more specific examples in the explanatory materials and OAIC guidance."[4]

[1] Proposal 4.1, p. 27, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[2] Proposal 4.2, p. 29, ibid
[3] Proposal 4.4, p. 35, ibid
[4] Proposal 4.2, p. 29, ibid

1.8. We remain concerned that the inclusion of a non-exhaustive list dilutes the principles-based and contextual approach to the definition of 'personal information' that, we submit, is essential. Such a list is also unlikely to withstand the rapid dynamic evolution of technical data and online identifiers and risks becoming outdated relatively quickly. Moreover, independent of educational efforts undertaken by the OAIC and others, such a list bears the risk of creating confusion among consumers who may believe that the listed types of information always constitute personal information. For example, as the Report notes it is not always the case that a phone number will be personal information – "[a] phone number as a bare set of numbers is not personal information. It is only when it is linked to an individual that the numbers fall within the definition.[5]"

1.9. If a list were included, it should be made clear in the legislation itself and the Explanatory Memorandum that the information on the list must still satisfy the primary elements of the definition, and that it will depend on the current context (noting the definition of and guidance in relation to de-identification) as to whether the information actually constitutes personal information in the specific circumstances. Noting our concerns above, the list ought to be drafted in a technology-neutral and sufficiently flexible manner.

'De-identified' information

1.10. Proposal 4.5 suggests to

> *"Amend the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, applied to personal information that involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context."*[6] *[emphasis added]*

1.11. It will be key for regulated entities to have clear guidance as to what constitutes 'current context' with respect to the risk of re-identification of previously de-identified information.

1.12. It will also be necessary for clear guidance to be provided as to what is required of regulated entities in relation to the definition for non-identifying information and pseudo-identifiers that relate to an individual, but of themselves do not identify the individual and require one or more additional pieces of information to identify a specific individual. Many technical identifiers and items of metadata are likely to fall into this category.

1.13. A relevant Oxford English dictionary definition of 'identify' includes both:

- *"Establish the identity of; establish who or what a given person or thing is"; and*
- *"recognise"*.

1.14. Taking the meanings 'establish the identity of' and similarly 'establish who or what a given person or thing is' leaves open the question "To what extent?" Is it necessary to know a person's name, address, personal history and/or likeness before they have been identified? Is it necessary to have sufficient information that they might be found or spoken to? In contrast the meaning 'recognise' suggests that someone is identified only if they can be associated with a previous encounter or engagement.

1.15. A relevant Oxford English dictionary definition of 'identity' is

> *"The condition or fact of a person or thing being that specified unique person or thing. esp., as a continuous unchanging property throughout existence; the characteristics determining this; individuality, personality."*

[5] p. 31, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[6] Proposal 4.5, p, 37, ibid

Accordingly, reference to the identity of an induvial can mean either or both that we know their characteristics and/or it can mean just that we can isolate them as a unique person.

1.16. The different meanings of 'identify' and 'identity' are discussed in section 4.3 of the Report (p. 31). Paragraphs 1, 2, 3, 4 and 5 seem consistent with the above, stating that an individual is identified when they are *"distinguished from all others in a group"*[7], whereas the sixth paragraph refers to OAIC guidance which requires that the unique identifier *"is able to be linked with other information that could ultimately identify the individual."*[8]

1.17. In our view, this proposition asserted in the sixth paragraph is controversial and probably incorrect. Consider, for example, an individual whose browser has accepted a cookie from an online shopping site. The shopping site may hold no information about the user other than their browsing and shopping habits as associated with the cookie. The information held is 'about' or 'relates to' a single unique individual who has been distinguished from all others, but it could not be used to 'ultimately identify the individual'. On the basis of the analysis in the sixth paragraph of section 4.3, the fact that individual has been distinguished from all others and profiled does not create personal information because the information collected is not capable of 'ultimately identifying' the individual. This outcome is inconsistent with international practice (express opt-in for cookies required by the GDPR), requires a particular and debatable meaning of 'identify' in the definition of personal information and appears to work against the policy of the objectives of the Act because it allows individuals to be distinguished, managed and targeted (though note our commentary at section 7 below) as long as the information collected cannot not be used to 'ultimately identify' the individual. The argument put in the sixth paragraph of section 4.3 of the Report also adds unnecessary complexity.

1.18. This issue has significant practical consequences for the communications industry. Take, as an example, a device identifier (e.g., International Mobile Equipment Identity (IMEI)) of a smartphone used to access internet sites and apps.

Some operators of internet sites and providers of apps may be able to associate a device identifier with a user, because they hold other identifying information about that user. For example, where an operator/provider has a user's site registration details: it may be reasonably practicable for that entity to deduce the user's identity from the identifier of a smartphone that the user uses to log on to and access the site/app; and accordingly, the device identifier of that user's smartphone may be identifying information in the site's operator's/provider's hands, and therefore personal information of that user.

Often, however, operators of internet sites and providers of apps will:

- not hold other identifying information about a user, e.g., where the user is a casual site user and has not provided any other details to the operator so the operator has no ability to associate a smartphone device identifier with an identifiable user; and/or
- only use the identifier to manage and deliver the service without collecting any information that is 'about' the user but could be said to 'relate to' the user.

In this context it is not reasonably practicable for that operator to infer the user's identity, so the device identifier of that user's smartphone is not identifying information in that operator's hands, and, therefore, on the basis of the analysis expressed in the Report at the sixth paragraph of section 4.3, is not personal information.

[7] p. 31, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[8] ibid

1.19. If the Act is amended to make it clear that an individual is identified when they are distinguished from all others (whether or not there is other information capable of ultimately identifying the individual) and that regulated personal information is information that 'relates to' an individual, we recommend that technical and process information that is necessary (for technical and processing purposes) but not relevant to individual privacy be expressly excluded.

1.20. If it is made clear that the information is not personal information unless this information actually is identifying the individual (in the sense of ultimate identification) or is linked to information capable of so identifying the individual, in determining whether an individual's identity may be inferred from non-identifying information, regulated entities should be required to consider and assess the security and access controls and other controls and safeguards applied to a data processing environment ('data situation') in which that data is handled, and the nature of the data. If the technical, operational, and legal controls and safeguards applicable to the data processing environment assure that identification risk is mitigated to the point where the risk of identification of individuals is very low, the information within this environment should be regarded as appropriately de-identified, and not constituting personal information.

By contrast, other data environments operated by or for a regulated entity may involve collection and handling of information that is on its face personally identifying: information (e.g., the names and addresses of individuals). Information within these other data environments would be personal information.

1.21. Each data situation should be assessed separately, with that assessment also considering whether the technical, operational and legal controls and safeguards applicable to each data processing environment are such as to assure that the risk of linkage or other association of information across separate data environments has been appropriately mitigated.

1.22. Against this background and taking into account the proposed definition and the criterion of 'current context' in particular, we believe that much of the technical information that participants in the communications sector (this includes, for example, carriage service providers, digital platforms and search engines) hold (and produce in the course of their normal operations, engagement with customers and service provision) should not be considered personal information unless it is linked (e.g., via account details) to a specific individual.

1.23. It is also worth noting that the Report summarised submitters' concerns that:

"Requiring consent in additional circumstances would lead to 'consent fatigue': where the individuals are overwhelmed with the number of consent requests they receive and, are less able to effectively engage with those consents"[9]

1.24. While the Report does not propose to extend the circumstances in which consent is required, the proposed amendment of the definition of personal information and inclusion of technical identifiers may result in a substantial (if not vast) increase of situations where consent may need to be sought as new classes of personal information are being created. This again highlights the need for clear guidance on the application of the definition of de-identification to avoid an over-expansion of the definition of personal information, and the need for appropriately crafted exceptions (also refer to our comments at section 5 below).

1.25. With respect to the scope of Proposal 4.6 to take reasonable steps to protect de-identified information from misuse, interference, loss and authorised re-identification, access modification or disclosure, we note the following:

The extension broadly copies the existing APP 11.1, however, it extends the APP from personal information to de-identified information.

[9] p. 102, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023

1.26. However, based on the risk the Report indicates it is trying to mitigate, we think the extension of privacy protections under APP 11 to de-identified information should be limited to the extent necessary to deal with the risk of harm to individuals which is likely to result from unauthorised re-identification. The risk of harm from unauthorised re-identification will depend on (1) the level of de-identification performed by an entity and (2) the nature of the de-identified information that was re-identified. Depending on these two factors will determine the reasonable steps that need to be taken.

Amended definition of 'collects'

1.27. The Report proposes to

"Amend the definition of 'collects' to expressly cover information obtained from any source and by any means, including inferred or generated information."[10]

1.28. We submit that the proposed definition of 'collects' is substantially too broad in scope as it would capture web crawling activities, e.g., activities to train AI or to develop an index for a search engine.

1.29. Consequently, we recommend amending the proposed definition to make clear that collection in this context requires 'holding' the data in a 'record', with the respective definitions of 'holding' and 'record' as currently contained in the Privacy *Act 1988* (Act). (Currently, an APP entity does not 'hold' personal information under the Act unless the entity maintains possession and control of a 'record' containing the information. A 'record' does not include a 'generally available publication', which is defined in the Act as a publication which is generally available to members of the public.)

Expanded definition of sensitive information

1.30. The Report proposes the following amendments in relation to sensitive information:

"Sensitive Information

(a) Amend the definition of sensitive information to include 'genomic' information.
(b) Amend the definition of sensitive information to replace the word 'about' with 'relates to' for consistency of terminology within the Act.
(c) Clarify that sensitive information can be inferred from information that is not sensitive information."[11]

1.31. As highlighted by many submitters throughout the process, alignment with other jurisdictions, where reasonably possible, is desirable to minimise the burden of compliance for regulated entities and confusion for individuals.

1.32. Consequently, we submit that the definition should not be amended to include 'genomic' information. Instead, the definition should be amended to reflect the language already used under the EU *General Data Protection Regulation* (GDPR) requirements for 'Processing of special categories of personal data' (the equivalent of the Australian 'sensitive information' concept) which includes:

"[…] the processing of genetic data [and] biometric data for the purpose of uniquely identifying a natural person"[12]

1.33. Irrespective of the language used in the GDPR and without wanting to claim expertise in the field of genomics, it may be the case that the term 'genomic' does not

[10] Proposal 4.3, p. 30, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[11] Proposal 4.9, p. 45, ibid
[12] Art. 9, para 1, Regulation (EU) 2016/679 (General Data Protection Regulation)

appropriately capture the intent of the proposed amendment. The World Health Organization distinguishes genetics and genomics as follows:

"Genomics is distinct from genetics. While genetics is the study of heredity, genomics is defined as the study of genes and their functions, and related techniques. The main difference between genomics and genetics is that genetics scrutinizes the functioning and composition of the single gene where as [sic] genomics addresses all genes and their inter relationships in order to identify their combined influence on the growth and development of the organism."[13]

While experts in the health sector may be better placed to comment, it also appears to us that information pertaining to the single genes (consider, for example the gene that is, if mutated, responsible for the occurrence of albinism), rather than only the whole genome, ought to fall under the new definition, in order to fully capture its intent.

2. Privacy policies and collection notices

Collection notices

2.1. Proposal 10.2 suggests that

"The list of matters in APP 5.2 should be retained. OAIC guidance should make clear that only relevant matters, which serve the purpose of informing the individual in the circumstances, need to be addressed in a notice.

The following new matters should be included in an APP 5 collection notice:

- *if the entity collects, uses or discloses personal information for a high privacy risk activity – the circumstances of that collection, use or disclosure*
- *that the APP privacy policy contains details on how to exercise any applicable Rights of the Individual, and*
- *the types of personal information that may be disclosed to overseas recipients."*[14]

2.2. The Report also proposes to update APP 5 to require collection notices to be *"clear, up-to-date, concise, and understandable"*[15]. We note the Discussion Paper proposed to reduce the list of matters to be covered in privacy collection notices. However, the Report now proposes to keep the full current list and include additional matters. Moreover, the Report proposes to extend the contents of privacy policies (refer to the Note at Proposal 10.2 and the respective chapters).

2.3. It will be difficult for entities to be able to provide concise notices if the proposed new matters are required to be included in collection notices.

2.4. While we understand the intent of the proposals concerning collection notices and agree with the recommendation not to further extend the circumstances that would require consent, we are concerned that the same information overload that leads to 'consent fatigue', i.e., 'collection notice fatigue' may occur, particularly, when notices become increasingly lengthy.

Standardised templates

2.5. The Report recommends that

[13] World Health Organization, as accessed at: https://www.who.int/news-room/questions-and-answers/item/genomics#:~:text=The%20main%20difference%20between%20genomics,and%20development%20of%20the%20organism on 14 March 2023
[14] Proposal 10.2, p. 99, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[15] Proposal 10.1, p. 97, ibid

"Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP Codes that may apply to particular sectors or personal information-handling practices."[16]

2.6. Standardisation through templates, icons or other means may be useful for some entities to assist with compliance. We agree that they may also assist individuals in understanding the content of notices and policies. However, standardisation of policies and notices will be less useful if the mandatory content is overly lengthy (see our comments at paragraphs 2.1 to 2.4 and section 8.12 to 8.15.)

We agree with the proposal that any standardisation should be developed by reference to relevant sectors, and, if standardised templates were to be developed, we welcome early engagement with all relevant stakeholders. The approach would need to be carefully undertaken to ensure that complex concepts are not oversimplified, particularly in technical sectors such as communications.

2.7. However, the use of standardised templates and layouts ought to be voluntary. If mandatory, standardised polices and notices would impede the ability for organisations to be innovative as to how they best present the information in their given context and to their particular audience.

For example, the delivery of information to inform a consent choice in the context of a search engine is likely to be very different from what may be most appropriate for a social media platform or a provider of mobile communication services.

2.8. Prescriptive requirements regarding the use of specific words or icons in Australia may make it difficult for companies with a global operating footprint to use consistent notices across jurisdictions. This may result in inefficiency, without delivering material benefits for Australian consumers. The interests of Australian consumers likely will be best served by giving companies freedom to determine how best to explain their services to consumers.

2.9. Consequently, we caution against prescriptive mandatory requirements for specific templates, layouts, terminology or icons. If standardised templates, icons etc. are developed, these must be voluntary.

3. Consent and Online Privacy Settings

Definition of Consent

3.1. The Report proposes to

"Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous."[17]

3.2. We support this proposed reform as set out in Proposal 11.1.

Fair and Reasonable Test

3.3. Proposal 12.1 recommends to

"Amend the Act to introduce a requirement that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances.

[16] Proposal 10.3, p. 100, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[17] Proposal 11.1, p.104, ibid

It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person."[18] [emphasis added]

3.4. The Act currently requires that personal information can only be used and disclosed for the purpose for which it was collected, or if used or disclosed for a secondary purpose, if that purpose is related to the primary purpose (for non-sensitive information) and the individual would reasonably expect their information to be used or disclosed for that purpose.

3.5. Proposal 12.1 recommends the introduction of an additional test that the handling of information be 'fair and reasonable in the circumstances'. We support changes to the Act that promote fair and reasonable handling of personal information.

3.6. If a fair and reasonable test is introduced, we agree with the proposed approach that the legislated factors of the fair and reasonable test are interpretative considerations only. We encourage the provision of high-level guidance in the Explanatory Memorandum to the Act and the development of more detailed OAIC Guidance and/or checklists, in close consultation with industry, to inform and give assurance to entities on how the test is to be interpreted.

3.7. Importantly, we believe, as also noted in various places within the Discussion Paper and Report, that further alignment of the Act with international privacy legislation regimes will be beneficial.

Against the Australian background of consent for lawful processing, we highlight that the GDPR standard of consent operates independent of other bases for processing, including:

"[…] legitimate interests pursued by the controller or third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data […].[19]

3.8. Therefore, we recommend consideration be given to further harmonise Australia's privacy framework with the GDPR in this respect to allow for additional bases for processing data and thereby reducing the compliance burden on Australian APP entities.

<u>Guidance on Consent Requests</u>

3.9. Proposal 11. 2 states that

"The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing standardised consents as part of any future APP codes."[20]

3.10. Similar to our feedback on standardised templates for policies and collection notices at section 2.5 to 2.9 above, we highlight that consent models will vary across online services due to the different types of services that are made available online and the different contexts in which consent can and should be obtained. In any case, we strongly recommend that any standardised consent notices for online services remain voluntary and welcome any OAIC guidance in this regard.

However, as with Proposal 10.3, overly prescriptive requirements may not be in the best interests of consumers, particularly if it leads to consent notices that are broader than they have to be, or that do not accurately reflect the way a particular APP entity wishes to use an individual's personal information. APP entities should be able to design

[18] Proposal 12.1, p. 116, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[19] Art. 6, para 1(f), Regulation (EU) 2016/679 (General Data Protection Regulation)
[20] Proposal 11.2, p. 106, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023

their own consent processes that best fits their own business, so long as they satisfy the stricter consent standard contemplated under proposal 11.1 (i.e., consent must be voluntary, informed, current, specific and unambiguous).

Online Privacy Settings

3.11. Proposal 11.4 recommends that

"Online privacy settings should reflect the privacy by default framework of the Act.

APP entities that provide online services should be required to ensure that any privacy settings are clear and easily accessible for service users."[21]

3.12. We warmly welcome the proposal for APP entities to ensure clarity and ease of accessibility for privacy settings. However, it is unclear if the intention of this proposal is that the strictest privacy settings be enabled by default. This approach would be unworkable and not in the interest of many consumer cohorts. It will be important to ensure that mandatory defaults do not put Australia out of step with other international privacy frameworks. It is indeed more appropriate to make privacy setting clear and easily accessible, and to enable individuals to set privacy protecting features to their desired level, including the most restrictive level.

Organisational accountability

3.13. Proposal 15.1 An APP entity must determine and record the purposes for which it will collect, use and disclose personal information at or before the time of collection. If an APP entity wishes to use or disclose personal information for a secondary purpose, it must record that secondary purpose at or before the time of undertaking the secondary use or disclosure.

3.14. This requirement will place a large, costly and unnecessary administrative burden on entities with limited or no privacy benefit to individuals. It is unnecessary for entities to invest in new processes to keep such internal records where this information is already required by the transparency obligations in APP 1 and privacy collection notice requirements in APP 5.

4. Children's privacy

Children's Online Privacy Code

4.1. At Proposal 16.5, the Report recommends to

"Introduce a Children's Online Privacy Code that applies to online services that are 'likely to be accessed by children'. To the extent possible, the scope of an Australian children's online privacy code could align with the scope of the UK Age Appropriate Design Code, including its exemptions for certain entities including preventative or counselling services.

The code developer should be required to consult broadly with children, parents, child development experts, child-welfare advocates and industry in developing the Code. The eSafety Commissioner should also be consulted.

[…]."[22]

4.2. We welcome the use of the *UK Age Appropriate Design Code* as the primary reference for a future Australian Children's Online Privacy Code. Any new code should be aligned in both scope and substance with international precedents in order to avoid

[21] Proposal 11.4, p. 109, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[22] Proposal 16.5, p. 157, ibid

causing issues for organisations that operate on an international basis. We look forward to engaging with the OAIC, the AGD and all relevant stakeholders on the development on this important piece of work.

4.3. We also refer to our comments in relation to the proposed requirements on a code developer in circumstances where it is unlikely that (an) industry association(s) can be found to develop a privacy code (refer to section 13 below).

4.4. In any case, we urge Government to engage industry in early and meaningful consultation to ensure that a Children's Online Privacy Code harmonises with existing and future regulatory and legislative processes in adjacent areas such as the Online Safety Codes for Class 1A and 1B (and Class 2) material and the Age Verification Roadmap, and initiatives taken to protect children's privacy by individual organisations.

People experiencing vulnerability

4.5. The Report proposes to

"Introduce, in OAIC guidance, a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information."[23]

And that:

"OAIC guidance on capacity and consent should be updated to reflect developments in supported decision-making."[24]

4.6. We welcome OAIC guidance that would clarify the circumstances when individuals may be experiencing vulnerability in relation to an increased risk of interference with their privacy.

4.7. The privacy of individuals who may be experiencing vulnerability must be protected, without measures requiring or allowing for additional disclosure of personal information. APP entities must not be required to proactively ascertain whether an individual, including a child, may be experiencing vulnerability as this would create additional privacy risks.

5. Rights of the individual

Right to access

5.1. Proposal 18.1 proposes to

"Provide[s] individuals with a right to access, and an explanation about, their personal information if they request it, with the following features:

(a) an APP entity must provide access to the personal information they hold about the individual (this reflects the existing right under the Act)"
[…].[25]

5.2. We support the existing right of access to personal information.

5.3. However, the proposed amendment of the definition of personal information broadens the definition, adding substantial complexity concerning technical identifiers and metadata, as highlighted in our commentary at section 1 above.

[23] Proposal 17.1, p. 162, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[24] Proposal 17.2, p. 164, ibid
[25] Proposal 18.1, p. 172, ibid

5.4. Depending on the interpretation (refer to the discussion on 'current context') of personal information, the retrieval of some types of personal information will be impractical, very difficult and costly for some of our members, and may be of limited benefit to the requesting individual.

5.5. The Singapore *Personal Data Protection Act 2012* (Schedule 5) recognises this difficulty and, accordingly, provides for an exception to the access in circumstances where "the burden or expense of providing access would be unreasonable to the entity or disproportionate to the individual's interest".

5.6. Equally, section 44 (Responding to IPP6 Request) of the *New Zealand Privacy Act 2020* provides for an exemption to access where personal information is not 'readily retrievable'.

5.7. With respect as to what constitutes 'readily retrievable', the New Zealand Office of the Privacy Commissioner (OPC) advises:

"There are a number of things to consider when determining whether information is readily retrievable, including the amount of time and cost required to retrieve the information, when the information dates from, and the manner in which the relevant information is stored.

A lot of information is technically 'retrievable', but this isn't necessarily the same as being 'readily' retrievable. For instance, even if information has been deleted from a computer, it can often be retrieved. Doing so, though, is often difficult, is a specialist job, and can be very costly. The results may also be imperfect, particularly if the information has been deleted some time ago.

It may also be difficult to retrieve physical documents, particularly if they date back a long way and the records of where the information is stored are not clear. Agencies need to try their best to get information for requesters, but there is only so far that they can reasonably be required to go."[26]

5.8. Consequently, we urge Government to amend the exceptions to access to personal information in APP 12 to similarly provide an exception where the burden or expense of providing access would be unreasonable to the entity or disproportionate to the individual's interest.

<u>Right to object</u>

5.9. The Report proposes to

"Introduce a right to object to the collection, use or disclosure of personal information. An APP entity must provide a written response to an objection with reasons."[27]

5.10. We believe that the scope of the right should be more clearly defined to apply to specific activities or circumstances of the processing, consistent with the corresponding right under GDPR, Article 21, which gives individuals the right to object, on grounds relating to their particular situation, "*unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.*"[28]

5.11. This may mitigate the impacts on entities responding to objection requests in legitimate circumstances (e.g., when processing is necessary to deliver a service under a contract).

[26] New Zealand Office of the Privacy Commissioner, as accessed at: https://privacy.org.nz/further-resources/knowledge-base/view/261?t=101292_142086 on 18 March 2023
[27] Proposal 18.2, p. 173, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[28] Art. 21, para 1, Regulation (EU) 2016/679 (General Data Protection Regulation)

5.12. We highlight the need to align with other relevant legislation, in particular the GDPR. Accordingly, we also recommend that any requirements regarding the right to object should only apply to an entity that has effective control over the information.

5.13. In addition, objection requests ought also to be subject to the 'frivolous and vexatious' test currently already applied under APP 12.

Right to erasure

5.14. At Proposal 18.3, the Report seeks to

"Introduce a right to erasure with the following features:

(a) An individual may seek to exercise the right to erasure for any of their personal information.
(b) An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort.
(c) In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement."[29]

5.15. We highlight that appropriate exceptions are necessary to balance any benefits for individuals with the potentially significant, costs and (im)practicalities of compliance for APP entities especially due to the proposed change to the definition of personal information. Consequently, any right to erasure must be qualified by well-defined pragmatic exceptions, including those recommended at Proposal 18.6 and extend to situations:

(a) where erasure is technically impractical, impossible or would constitute an unreasonable burden to action;
(b) where the information serves the entities legitimate interests in relation to operations, service quality, maintenance and network assurance activities, safety and security (such as, but not limited to, cyber security); and
(c) where a request is frivolous or vexatious.

5.16. We are very concerned with and unclear as to how the proposed right to erasure would operate in relation to a customer's right to complain or commence proceedings – and the APP entity's need to potentially respond to the complaint – to the Telecommunications Industry Ombudsman (TIO), OAIC or other regulators. Once customers have requested the erasure of their data (and entities have complied to the extent permitted and/or technically feasible), we would expect that a customer could no longer make a complaint that relates to (and not necessarily only confined to) any data that has been erased, as the APP entity would not be in a position to provide a meaningful response in relation to the complaint.

Similar considerations would apply in relation to complaints to other regulators or the OAIC.

5.17. It is also important to understand that many of the efforts undertaken by our industry in relation to providing a safer online experience, including measures proposed in the draft Consolidated Industry Codes of Practice for the Online Industry, Phase 1 (class 1A and class 1B material) rely on personal information (particularly if the definition of personal information was to be amended as proposed).

Erasure of personal information could, therefore, impact a user's online safety experience and an APP's entity ability to comply with the measures as currently

[29] Proposal 18.3, p. 176, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023

proposed in the draft codes that have been submitted for registration to the eSafety Commissioner.

5.18. In relation to item (c) of the proposal, section 18.5.1 of the Report states that the Australian Federal Police (AFP) considered metadata as one of the categories that may warrant special treatment under any right to erasure, i.e., quarantining rather than erasure to allow continued access for law enforcement.[30] The Report notes:

"The AFP suggested that these types of information could be quarantined rather than erased as an option to comply with the right.[1529] This approach has merit. Applying the right to erasure to require quarantine of information in the above categories would operate to ensure such information is available to law enforcement if required but would still restrict the entity's own use of the information. The quarantine exception would not be a requirement to retain information; entities would not need to hold information longer than they normally would in line with their normal destruction processes."

[1529] Submission to the Discussion Paper: AFP

5.19. It is important to understand that the ability to quarantine information out of a very large pool of information (metadata) may involve substantial changes to current systems and processes and, consequently, costs to develop. If it is technically impractical or unreasonably burdensome to quarantine the information retained for complying with the mandatory data retention laws, then this should be an exception to the right to erasure.

5.20. In the context of quarantining, we recommend that further consideration is given as to the definition of 'quarantining' as this term can have different meanings in a technical context, i.e., 'logical quarantining' vs. 'virtual quarantining' etc. We urge Government to consult with technical industry experts on this matter.

5.21. Further, should a right to erasure be introduced, it should as far as possible be aligned with the equivalent right under the EU GDPR in order to promote harmonised international standards and minimise any compliance burden on APP entities that have already updated their systems to comply with the GDPR requirements.

Right to de-index internet search results

5.22. Proposal 18.5 proposes to

"Introduce a right to de-index online search results containing personal information which is:

(i) sensitive information [e.g. medical history]
(ii) information about a child
(iii) excessively detailed [e.g. home address and personal phone number]
(iv) inaccurate, out-of-date, incomplete, irrelevant, or misleading

The search engine may refer a suitable request to the OAIC for a fee.

The right should be jurisdictionally limited to Australia."[31]

5.23. We understand the intent of the proposal but remain concerned with the implications that the implementation of this proposal would have; namely, to make search engines the arbiter over whether certain content will be indexed or not. We do not believe that this is desirable.

[30] p. 175, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[31] Proposal 18.5, p. 179, ibid

Whether information is inaccurate, out of date, incomplete, irrelevant, or misleading is best determined by the author or webmaster of the underlying webpage which publishes the information, or if necessary, a court.

5.24. The Report suggests that Proposal 18.5 was drafted to reflect the test established by the 2014 decision of the Court of Justice of the European Union *in Google Spain SL v Costeja González* (Costeja Case), adapted for the Act. The test established by the Costeja case is:

"[…] that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible with Article 6(1)(c) to (e) of the directive because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased."[32] [emphasis added]

5.25. The proposal as drafted is, therefore, substantially different from – and going well beyond – the test established by the Costeja Case which confined itself to the erasure of "*inadequate, irrelevant or no longer relevant, or excessive*" information.

It is not appropriate to extend this already established test to further categories, especially those that would require a substantial amount of context and judgement, such as whether information is 'misleading'.

5.26. Especially in relation to the latter ('misleading'), we note that the 9 December 2022 public communiqué of the Standing Council of Attorneys-General included the in-principle approval of the amendments for *Part A of the Stage 2 Review of the Model Defamation Provisions* (subject to final agreement in the first half of 2023). Those include:

"Two conditional, statutory exemptions from defamation liability for a narrow group of internet intermediaries, including search engines in relation to organic search results"[33]

This proposed limited exemption from liability for defamation for search engines was agreed (in-principles) on the basis that the *"search engine's role in the process of publishing the matter is of a solely technical and automatic nature"*[34] and *"in performing its function, the search engine is content neutral"*[35].

In its deliberations to exempt search engines from defamation liability in relation to organic search results, it appears that the Meeting of Attorneys-General also gave consideration to the fact that search engines are unable to remove the content from the internet and that they are ill-placed to make judgements about the defamatory matter itself.

There will likely be many situations where an individual seeks de-indexing on the basis that information is 'misleading' while other individuals have a continued interest for that website to remain indexed.

It is concerning that search engines should now be placed in a similar position (arguably without the concern of defamation liability) to make judgements as to

[32] Judgment of the Court (Grand Chamber), 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, as accessed at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 on 19 March 2023

[33] Attorney-General's Department, as accessed at: https://www.ag.gov.au/about-us/publications/standing-council-attorneys-general-communiques on 19 March 2023

[34] p. 30, Meeting of Attorneys-General: Stage 2 Review of the Model Defamation Provisions Part A: liability of internet intermediaries for third-party content, Background Paper: Model Defamation Amendment Provisions 2022 (Consultation Draft), Aug 2022, as accessed at: https://www.justice.nsw.gov.au/justicepolicy/Documents/review-model-defamation-provisions/background-paper--for-draft-part-a-model-defamation-amendment-provisions-2022.pdf on 19 March 2023

[35] p. 30, ibid

whether information that 'relates to' a person is misleading when the underlying key rationale has remained unchanged.

5.27. With reference to the Costeja Case, it is also important to understand that the test established by the case only related to "*the list of results displayed following a search made on the basis of his name*".

However, as drafted, Proposal 18.5 would extend to any search made on the basis of any input parameter relating to a person, thereby extending the test further.

As drafted, a search made, say on the basis of a person's date of birth, which will potentially somewhere in the search results contain a link to a webpage containing personal information of the requesting individual. This link would need to be de-indexed even if that search result was listed at a very low rank with no reasonable likelihood of ever being surfaced through a search in a 'real life scenario', i.e., other than the requesting individual 'hunting' for the information.

6. Automated Decision Making

6.1. Proposals 19.1 to 19.3 deal with the types of personal information that will be used in substantially automated decisions that must be included in privacy policies, the high-level indicators of types of decisions that could constitute decisions with a 'legal or similarly significant effect', and a new right for individuals to request meaningful information about how automated decisions with legal or similarly significant effect are made.

6.2. We agree with other submitters' concerns that the term 'legal or similarly significant effect' does not provide sufficient certainty for APP entities in relation to their obligations and requires clarification. To avoid an overly broad interpretation, this requirement should be confined to decision making where the impact is on fundamental rights of individuals (e.g., housing, education, employment and other areas protected from discrimination under the law).

6.3. We also welcome the proposal (albeit not included in one of the proposals themselves) to undertake consultation "*to ensure the parameters of 'substantially automated' are appropriately calibrated.*"[36]

6.4. Any right for individuals to request information about substantially automated decisions should be accompanied with clear guidance about the types of information that entities are expected to provide to individuals. Importantly, it ought to be clear that to the extent individuals are entitled to request information about substantially automated decisions, this should not require the disclosure of proprietary or confidential information regarding algorithms or processes used to make those decisions. This would be particularly problematic where such processes are used to detect fraud or the misuse of services, as it may open the door for bad actors to circumvent these processes and abuse services.

7. Opt-outs, direct marketing, targeted advertising and profiling

7.1. The Report makes a number of proposals in relation to the definitions, right to opt out, requirements to obtain consent, information provision and other proposals with respect to direct marketing, targeting and trading (DMTT practices).

7.2. Some of the proposals put forward in the Discussion Paper were already far-reaching in that they did not, in our view, appropriately recognise the benefits of DMTT practices

[36] p. 191, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023

for consumers, either directly, or indirectly by providing free services in exchange for the use and processing of customer data for DMTT practices.

7.3. We are, therefore, very concerned that the Report goes even further beyond the matters discussed in the Issues Paper (Oct 2020) and the Discussion Paper by including new proposals that could, if implemented, have substantial impacts not only on digital platforms and data brokers, but across the Australian economy more broadly.

7.4. We appreciate the intention to provide individuals with more control over their personal information and how it is being used, especially in the context of today's digital economy. However, we believe that the proposals put forward in the Report do not strike the right balance between enhanced privacy protections and business needs.

As currently drafted (intentionally or unintentionally), they also fail to recognise the complex nature of data use (including of de-identified data) and the prevalence and benefit of service personalisation in our economy. They also do not recognise that many companies have voluntarily established measures to give consumers transparency and control over their information. We believe further work will be required to develop more practical proposals.

7.5. For the purpose of our submission, we will limit our feedback on Proposals 20.1, 20.3, 20.6 and 20.8.

Definition of direct marketing, targeting and trading, the unqualified right to opt-out of targeted advertising and additional requirements on targeting

7.6. The Discussion Paper included a number of proposals relating to direct marketing and targeting. Drawing on these and submissions received in response to the Discussion Paper, the Report sets out a number of proposals in Section 20. The first is to proposes to introduce definitions for 'direct marketing', 'targeting' and 'trading':

"***Direct marketing*** *– capture the collection, use or disclosure of personal information to communicate directly with an individual to promote advertising or marketing material.*

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

Trading *– capture the disclosure of personal information for a benefit, service or advantage."*[37]

7.7. The Report also proposes to

"*Provide individuals with an unqualified opt-out of receiving targeted advertising."*[38] [emphasis added]

Further, the Report introduces the requirement that an individual's consent must be obtained to trade their personal information (Proposal 20.4).

7.8. In addition, Proposal 20.8 seeks to introduce general requirements:

"*Amend the Act to introduce the following requirements:*

- *Targeting individuals should be fair and reasonable in the circumstances.*
- *Targeting individuals based on sensitive information (which should not extend to targeting based on political opinions, membership of a political association or*

[37] Proposal 20.1, p. 211, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[38] Proposal 20.3, p. 214, ibid

membership of a trade union), should be prohibited, with an exception for socially beneficial content."[39]

7.9. These proposals raise a number of concerns:

First, the proposed definitions of 'targeting' regulates non-personal information that is incapable of being tied to an identified person. Subject to our comments in paragraphs 1.10 to 1.24 (sub-section on de-identified information), this is inconsistent with the policy intent that underlies the Act which is to protect information that is personally identifying.

Importantly, the inclusion of de-identified information and un-identified information in the definition means that very limited categories of information are excluded from the definition.

The inclusion of de-identified and unidentified information in combination with the definition of 'targeting' (refer to our commentary further below) would mean that many services (for example those that use technical identifiers) would no longer be able to be provided once an individual chooses to exercise their unqualified right to opt out of 'targeted advertising'.

7.10. Second, the definition has, compared to the proposals contained in the Discussion Paper, now been extended to capture all 'tailoring online services, *content, information, advertisements or offers*' instead of 'only' services providing personalised advertising.

As *"In any Act where a word or phrase is given a particular meaning, other parts of speech and grammatical forms of that word or phrase have corresponding meanings."*[40], therefore, Proposal 20.3 to provide an unqualified opt-out for targeted advertising is not only limited to advertising but, in fact, extends to all the activities listed under the definition of 'targeting', i.e. tailoring online services, content, information, advertisements or offers' – and applies to all types of data (note our comments above.)

It is not clear how the opt-out right would operate in practice as individuals would most likely not understand what they had opted out of – advertising only or all tailoring online services, content, information, advertising and offers.

7.11. The implications of capturing all 'tailored online services *content, information, advertisements or offers*' – especially if viewed in combination with the inclusion of de-identified information in the definition of targeting – are fundamental.

Essentially, the proposal means that almost any type of data set (given the inclusion of de- and un-identified data) cannot be used (once opted out) for the delivery of any service, noting that the definition goes beyond advertising

This would lead to scenarios that appear detrimental to consumers. It appears to be based on speculation about possible harms without genuine evidence.

7.12. Third, the proposals neglect the benefit that personalised services have to consumers, small business, Government and the Australian economy more broadly. Care must be taken to ensure that additional regulations do not prohibit or constrain general service customisation and personalisation, which are largely beneficial to consumers.

Therefore, it is key to understand that an unqualified right to opt-out could raise the cost and lower the effectiveness of advertisements, noting current inflationary pressures. For example:

- Personalisation makes it far more efficient for small businesses to find customers and grow their business. A recent report by Deloitte found 71% of Australian small

[39] Proposal 20.8, p. 219, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[40] Section 18A, *Acts Interpretation Act 1901 (Cth)*

businesses using personalised advertising reported it is important for the success of their business.[41]

- Similarly, charities and not-for-profit organisations make use of personalised advertising for lack of resources on more generalised (usually more expensive) forms of advertising. Further, charities use personalisation to break through 'compassion fatigue', to determine which social causes users are most likely to align with.[42]
- Government advertising strategies rely heavily on targeting specific cohorts for advocacy and awareness. For example, 17% of the Australian Electoral Commission's awareness campaign budget was dedicated to reaching culturally and linguistically diverse (CALD) and indigenous communities.[43] Political parties, advocacy groups and agencies (such as the Australian Electoral Commission) will experience difficulty in engaging with users based on their interests or demographics, most notably in the lead up to events of national or political importance such as referendums or elections, were the right being exercised.

7.13. We note that the implementation of an opt-out of targeted advertising as drafted would have practical limitations. For example, once a customer A opts out of receiving targeted advertising, an entity can no longer use un/de-identified data to target that customer. However, because of the broad definition of targeting and un/de-identified information, if that entity were to use un/de-identified data of individuals who viewed services on that entity's website to display an advertisement specifically in relation to what the customer has viewed on that website, it would be very difficult or impossible for that entity to prevent that advertisement from appearing for customer A unless customer A was always using the same device identifier that the entity knew about. If customer A used a different device (with, therefore, a different device identifier), the entity would not know that the IP address was associated with customer A to prevent the target advertising from occurring.

7.14. Fourth, it is even more important to highlight the effect that a broad opt-out right, as currently drafted, could have on the general fabric of the internet.

7.15. The Report does not only include an unqualified right to opt-out of receiving targeted advertising but, importantly, makes clear that:

"Importantly, opting out of receiving targeted advertising should not be a barrier to service for individuals who elect to make this choice. Given the availability of other forms of advertising, such as contextual advertising, access to a service should not be made conditional on consenting to receiving targeted advertising."[44]

7.16. Essentially, this inability not to serve individuals who opt out risks substantially increasing the share of internet experiences/services on the internet being located behind a pay-wall as ad-supported business models could no longer provide their services for free.

Whiles so many services on the internet are free, they are not free to develop or maintain. It is also incorrect to assume that service providers can easily just continue to provide the remaining parts of the service that has not been opted-out or the aspects of the service that are, in the eyes of the individual, not affected by the opt-out. When the provider set up systems and processes, or calculated a business plan, it may have

[41] Deloitte, 'Dynamic Markets Report: Australia - unlocking small business innovation and growth through the personalised economy', *Meta Australia blog,* October 2021, as accessed at: https://australia.fb.com/economic-empowerment/ on 19 March 2023

[42] C Green, 'What the next generation of personalisation means for charity marketing', *Charity Digital*, 19 August 2020, as accessed at: https://charitydigital.org.uk/topics/topics/what-the-next-generation-of-personalisation-means-for-charity-marketing-7831 on 19 March 2023

[43] Australian Department of Finance, 'Campaign advertising by Australian government departments and entities, 2021 - 2022', Commonwealth of Australia, 2022, as accessed at: https://www.finance.gov.au/sites/default/files/2022-12/Campaign%20Advertising%20by%20Australian%20Government%20Departments%20and%20Agencies%20-%20Report%202021-22.pdf on 19 March 2023

[44] p. 214, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023

done so with view to providing a whole service. We warn against the assumption that disaggregation of the service or service features is easily possible, if possible at all.

Consequently, the notion that services ought to be continued to be provided for free without the provider of the service receiving the benefit on which the business model was calculated that the service could be provided in the first place defies any economic and contractual theory and ought to be abandoned. A more nuanced approach would be required if a more practical, narrow opt-out right of specific targeted service personalisation approaches was to be proposed in the future.

7.17. Indeed, research has demonstrated that consumers value the trade-off that personalised advertising facilitates:

- A recent Ipsos report found 70% of consumers prefer to have free access to social media and mobile apps in exchange for seeing ads.[45]
- The OAIC's own *Australian Community Attitudes to Privacy Survey* also found that 58% of Australians agree it is fair they share some information if they want to use a digital service.[46]

7.18. Fifth, if APP entities were to be required to comply with an unqualified opt-out request in relation to targeted advertising (and direct marketing), and given the necessity to either place a service behind a pay-wall or to derive revenue from advertising in order to continue to make the service available for free, we could expect general advertising to increase if the proposal was to be implemented (and taken up by consumers).

7.19. The consequence would be that advertising would likely become more random and irrelevant, thereby degrading the user experience.

However, again, a number of studies highlight that consumers prefer personalised advertising over generalised advertising and are even willing to pay for ad-supported free services. Consider, for example, the following:

- In a report conducted by Infogroup, roughly 90% of people said that messages from companies that are not personally relevant to them are "annoying".[47] According to the OAIC's own *Australian Community Attitudes to Privacy Survey*, 48 per cent would prefer ads they receive to be targeted and relevant, with another 29% having no opinion on whether ads should be targeted or not[48].
- Further, an IAB paper found that there has been a $10.2 billion increase in consumer value from having consumption more closely matched to consumer preferences, plus savings of $36.5 billion annually for consumers due to decreased transaction costs.[49]

7.20. Sixth, especially in the context of digital platforms (and again against the background of an unqualified right to opt out whilst maintaining a requirement on the entity to continue to provide the service), tailored services help to prioritise content that a user will find most valuable amongst millions of posts/blogs etc. It could be said that some of

[45] Ipsos, Global ipsos survey for small enterprises, *Ipsos*, July 2022, as accessed at: https://www.ipsos.com/en-us/news-polls/small-medium-sized-businesses-leveraging-social-media-digital-tools on 19 March 2023
[46] Office of the Australian Information Commissioner, 'Australian Community Attitudes to Privacy Survey', p. 31, oaic.gov.au, Sept 2020, as accessed at: https://www.oaic.gov.au/__data/assets/pdf_file/0015/2373/australian-community-attitudes-to-privacy-survey-2020.pdf on 19 March 223
[47] Infogroup, The Power of Personalization, May 2019, https://www.emarketer.com/chart/228797/attitudes-toward-personalization-among-us-internet-users-jan-2019-of-respondents
[48] Office of the Australian Information Commissioner, 'Australian Community Attitudes to Privacy Survey', p. 31, oaic.gov.au, Sept 2020, as accessed at: https://www.oaic.gov.au/__data/assets/pdf_file/0015/2373/australian-community-attitudes-to-privacy-survey-2020.pdf on 19 March 223
[49] IAB, 'Ad'ing value: the impact of digital advertising on the Australian economy and society', PWC, November 2022, as accessed at: https://m.iabaustralia.com.au/asset/395:ading-value---the-economic-impact-of-australias-digital-advertising-industrypdf#:~:text=The%20value%20of%20advertising%20for,for%20businesses%20of%20different%20sizes on 19 March 2023

the most well-known digital platforms centre their services around this capability and the user's preference of such content prioritisation.

- A recent Ipsos report found that 82% of people who use Facebook agree that they like it when Facebook shows posts from friends that are relevant to them.[50]
- And a PwC Consumer Survey found that 78% of respondents indicate that digital services and content have enabled them to more easily stay in contact with friends and family – this share increased to up to 81% in regional areas.[51]

7.21. Seventh, restrictions on targeting would also impact Australia's ability to leverage the value of the global creator economy, as creators may be less able to grow their presence based on personalised or recommended experiences. In 2022, the creator economy was estimated to be worth as much as $150 billion[52], and 6 million people in Australia now consider themselves creators.[53]

7.22. We also note that the proposals fail to recognise the significant voluntary, industry-led work aimed at giving consumers greater transparency and control over the data that APP entities may be collecting or processing.

7.23. In the context of Proposal 20.2, Section 20 of the Report does not address a number of the ambiguities of the current Act that apply in relation to direct marketing. In particular, the Report does not indicate whether the specific direct marketing rules under APP 7 should be retained or discarded. If APP 7 is to be retained, then there are a number of aspects that ought to be clarified. For example, the treatment of inferred information under APP 7 is currently unclear in that it may be regarded as being self-generated and, therefore, collected from someone other than the individual themselves, in which case different compliance requirements apply (including consent requirements). The Discussion Paper had recommended repealing APP 7, given the introduction of more specific rules for direct marketing and targeting, which is an approach that would help eliminate ambiguity.

7.24. We urge the AGD to carefully re-consider the proposals of Section 20 that we consider substantially too far-reaching and, consequently, out-of-step with other international privacy protection regimes. More work is required to achieve a practical approach to give individuals more control over their information, including well-defined opt-out rights of some targeted activities.

Targeting Children

7.25. The Report proposes to

"Prohibit targeting to a child, with an exception for targeting that is in the child's best interests."[54]

7.26. This prohibition is, in our view, too broadly scoped and/or open to interpretation. We believe that it ought to only apply to commercial content, i.e., it should not apply to non-commercial recommendations, such as to music.

7.27. We would also welcome clearer guidance about what constitutes targeting that is in the child's best interests.

---

[50] Ipsos, Global ipsos survey for small enterprises, *Ipsos*, July 2022, as accessed at: https://www.ipsos.com/en-us/news-polls/small-medium-sized-businesses-leveraging-social-media-digital-tools on 19 March 2023

[51] PWC, PWC Consumer Survey, Nov 2022, as accessed at: https://m.iabaustralia.com.au/asset/395:ading-value---the-economic-impact-of-australias-digital-advertising-industrypdf#:~:text=The%20value%20of%20advertising%20for,for%20businesses%20of%20different%20sizes on 19 March 2023

[52] R Florida, 'The rise of the creator economy', *Creative Class Group*, Nov 2022, as accessed at: https://creativeclass.com/reports/The_Rise_of_the_Creator_Economy.pdf on 19 March 2023

[53] ibid.

[54] Proposal 20.6, p. 217, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023

8. Security, Destruction and Retention of Personal Information

The need for clearer security requirements – what are 'reasonable steps'?

8.1. We support Proposal 21.1. to state that 'reasonable steps' include technical and organisational measures.

Baseline security requirements

8.2. Proposal 21.2 suggests to

"Include a set of baseline privacy outcomes under APP 11 and consult further with industry and government to determine these outcomes, informed by the development of the Government's 2023-2030 Australian Cyber Security Strategy."[55]

8.3. We welcome the proposal that APP 11 should remain principles-based with a closer focus on desired outcomes rather than prescriptive requirements as to how these outcomes are to be achieved.

We also support a consultative approach for any baseline privacy outcomes in relation to APP 11.

However, we believe that such outcomes would be best dealt with in OAIC Guidance rather than the legislation itself to ensure sufficient flexibility in light of dynamic technology developments. This would also allow the OAIC to flexibly update Guidance in line with updated recommended steps by relevant bodies, such as the Australian Cyber Security Centre.

8.4. When applying the proposed baseline privacy outcomes, there should also be an express requirement to take account of the level of control that the APP entity in question has over the relevant information.

Guidance on Obligations under APP 11

8.5. Proposal 21.3 suggests to

"Enhance OAIC guidance in relation to APP 11 on what reasonable steps are to secure personal information. The guidance that relates to cyber security could draw on technical advice from the Australian Cyber Security Centre."[56]

8.6. We agree that the OAIC guidance could be enhanced to provide further information on what constitute 'reasonable steps' to secure personal information, with the OAIC drawing on the technical expertise of the Australian Cyber Security Centre.

8.7. In this respect, we are also conscious of the recent *2023-2030 Australian Cyber Security Strategy Discussion Paper* which canvasses additional protections for 'customer data', including through inclusion in the *Security of Critical Infrastructure Act 2018*.[57] We welcome further guidance as to how these two processes (and guidance/legislation) would interact.

8.8. We also believe that the level of control that an entity has over the relevant information ought to be expressly addressed in the requirements of APP 11.

---

[55] Proposal 21.2, p. 224, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[56] Proposal 21.3, p. 225, ibid
[57] p, 7, p, 17 and p. 24, Australian Government, Expert Advisory Board, *2023-2030 Australian Cyber Security Strategy Discussion Paper,* Feb 2023

Dealing with personal information that is no longer necessary

8.9. In line with our observations on guidance on the security of personal information and following through with the controller-processor concept, we also note that any guidelines in relation to the 'reasonable steps' that are expected of entities to destroy or de-identify personal identity personal information (at Proposal 21.5) ought to only apply to the entity that has control over the information.

Review legal provisions that require retention of personal information

8.10. At Proposal 21.6, the Report recommends

"The Commonwealth should undertake a review of all legal provisions that require retention of personal information to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information.

This further work could also be considered by the proposed Commonwealth, state and territory working group at Proposal 29.3 as a key issue of concern where alignment would be beneficial.

However, this review should not duplicate the recent independent review of the mandatory data retention regime under the Telecommunications (Interception and Access) Act 1979 and the independent reviews and holistic reform of electronic surveillance legislative powers."[58]

8.11. We wholeheartedly support this proposal, given our comments in relation to the manifold, often confusing, retention periods for data at section 8.12 to 8.15 below (Proposal 21.8). We also highlight it is necessary for regulators to be part of this review exercise.

However, we strongly urge the AGD not to scope the review too narrowly and to also include an examination of regulatory provisions (e.g., Codes) and practical requirements that arise from the need to respond to customer complaints, including those that have been escalated to regulators or external dispute resolution regimes (EDR), etc.

Increasing transparency for the retention of personal information

8.12. The Report proposes to

"Amend APP 1.4 to stipulate than an APP entity's privacy policy must specify its personal information retention periods."[59]

8.13. We do not support this proposal.

8.14. The appropriate retention period for any data depends on a range of factors that change depending on the data and the circumstances. A business may be required to keep data because for example:

- It is being used by the business to service the customer. Information required for an active service and customer relationship does not have a 'retention period'.
- It is listed as information that must be kept by law. There are various laws that apply to tax records, corporate registers, HR policies and records and some that apply specifically to the telecommunications sector (see below).
- It is required by the business for risk management purposes. This factor is influenced but not determined by limitation periods. For example, a business can be sued in

[58] Proposal 21.6, p. 227, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[59] Proposal 21.8, p. 229, ibid

tort for up to six years from the date on which the cause of action accrues. A prudent business might, therefore, keep records relating to a customer relationship for six years from the date of termination of the relationship. However, the business is not required to keep the records for this period, it is only the limitation period for possible legal action which might cause the business to maintain the record depending on their assessment of the risk.

- The business is on notice of a legal claim. It can be contempt of court and/or give rise to an adverse inference if evidence relevant to a dispute has been destroyed.

8.15. The retention periods for the various types of personal information that many sectors hold are manifold. Listing all retention periods is, therefore, contrary to the aim of having privacy policies that are not overly lengthy and still within the realm of what the average reader would consider acceptably 'digestible'. Listing these retention periods in an easily understandable manner will be equally challenging.

For example, in the telecommunications sector, personal information can be subject to different retention periods, depending on the underlying legislation and/or regulation, e.g., the data retention legislation under the *Telecommunications (Interception and Access) Act 1979*, the *Telecommunications Consumer Protections (TCP) Code*, ACMA regulations in relation to complaint handling etc. In addition, these retention periods can vary for different customer cohorts, for example, where customers are affected by financial hardship or domestic and family violence.

The proposal is not practical and does not provide, on balance, meaningful benefit to consumers and ought not to be progressed.

9. Controllers and processors of personal information.

Processor and controller distinction

9.1. Proposal 22.1 proposes to

"Introduce the concepts of APP entity controllers and APP entity processors into the Act.

Pending removal of the small business exemption, a non-APP entity that processes information on behalf of an APP entity controller would be brought into the scope of the Act in relation to its handling of personal information for the APP entity controller. This would be subject to further consultation with small business and an impact analysis to understand the impact on small business processors."[60]

9.2. We welcome the introduction of the concepts of APP entity controllers and APP entity processors into the Act. This recognition of the different roles that controllers and processors have in relation to personal information reflects the operational reality of many business relationships. This also affords consumers more clarity on the appropriate party to engage when exercising their rights.

9.3. Additionally, the controller – processor distinction will bring Australia more closely in line with other privacy regimes around the world and enable increased interaction among digital economies.

10. Overseas data flows

A mechanism to prescribe countries and certification schemes

9.4. We welcome the introduction of a mechanism to prescribe countries and certification schemes under APP 8.2(a). This would provide greater certainty on the overseas laws or

[60] Proposal 22.1, p. 233, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023

schemes that afford 'substantially' similar protection to the Act. Prescribing existing and well-established schemes would also allow business efficiency when operating globally while giving data a recognised standard of safeguarding. For this reason, we would support the prescribing the APEC Cross-Border Privacy Rules (CBPR) System under the proposed APP 8.2(a) and were encouraged to see this was highlighted in the Discussion Paper[61].

9.5. However, we recommend that Government undertake careful consideration to ensure this does not add unnecessary friction to data flows between countries. Australia has admirably been a longstanding champion of open data flows via the World Trade Organization and other multilateral fora, in recognition of the economic benefits that arise from digital trade. It would be concerning if a certification scheme became so restrictive as to signal to other countries in the Asia-Pacific region that data localisation measures are beneficial public policy goals.

9.6. The independent think tank Information Technology and Innovation Foundation (ITIF) found a direct link between restrictive data policies, lower economic productivity and increased prices. In a report published in July 2022[62], it found: ITIF developed a scale of data restrictiveness. Every additional point of being restrictive cut a nation's gross trade output 7 percent, slows its productivity 2.9 percent, and hikes downstream prices 1.5 percent over five years.

9.7. In the same vein, we encourage Government to recognise binding corporate rules (BCRs) as a valid cross-border data transfer mechanism. The GDPR currently recognises BCRs approved by a competent data protection authority in the EU as a mechanism for transfers of personal data outside the EU within a multinational group of undertakings or enterprises. This would materially support economic engagement with the EU (and other jurisdictions that recognise BCRs) by reducing regulatory burden while ensuring appropriate protection of personal information.

Standard contractual clauses

9.8. Proposal 23.3 suggest that

> "*Standard contractual clauses for use when transferring personal information overseas should be made available to APP entities.*"[63]

9.9. We would welcome such standard contractual clauses for voluntary use being made available. We recommend that those clauses ought to align with equivalent clauses used in the GDPR where possible, to ensure interoperability and to avoid entities being faced with multiple different standard contractual clauses from different jurisdictions.

Overseas disclosures

9.10. In relation to overseas disclosures we note that it is imperative that the Act retains the informed consent exception in APP 8.2(2) which recognises that an individual's consent is one of the several methods by which entities can transfer data internationally.

9.11. Further, we note that the Report proposes at Proposal 23.5 to

> "*Strengthen APP 5 in relation to overseas disclosures by requiring APP entities, when specifying the countries in which recipients are likely to be located if practicable, to also specify the types of personal information that may be disclosed to recipients located overseas.*"[64]

[61] Proposal 23.2, p. 238, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[62] Report accessible at: https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/
[63] Proposal 23.3, p. 238, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[64] Proposal 23.5, p. 242, ibid

9.12. The recommend that the Act should not require APP entities to notify individuals under APP 5.1 of the types of personal information that may be disclosed overseas. To the extent any such requirement is imposed, it should apply more narrowly and only to disclosures made in the course of seeking an individual's consent to disclose data to an overseas recipient.

9.13. At least, we recommend that a similar qualification of 'where practicable' as already present in relation to the recipient countries be also included in relation to the types of personal information that may be disclosed.

Definitions of 'disclosure' and 'use'

9.14. The Report proposes at 23.6 to

> *"Introduce a definition of 'disclosure' that is consistent with the current definition in the APP Guidelines."*[65]

9.15. We welcome the definition of 'disclosure' to provide more business certainty on the interpretation of the term. This is particularly relevant given there are currently different interpretations of the term 'disclosure' in various legal contexts.[66]

9.16. We also recommend that a definition of 'use' be introduced that is consistent with the current definition in the APP Guidelines. Ensuring that both terms are clearly defined is essential for business and legal clarity and for consistency with the existing APP Guidelines.

11. Direct right of action and statutory tort for serious invasions of privacy

Direct right of action

10.1. The Report recommends to

> *"Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy. The model should incorporate the appropriate design elements discussed in this chapter."*[67]

10.2. Proposal 26.1 is accompanied by the following design elements:

> *"The Act should be amended to permit individuals to apply to the courts for relief in relation to an interference with privacy with the following design elements:*
>
> *(a) The action would be available to any individual or group of individuals who have suffered loss or damage as a result of privacy interference by an APP entity. This would include claims by representative groups on behalf of members affected by breaches of the Act.*
> *(b) Loss or damage would need to be established within the existing meaning of the Act, including injury to the person's feelings or humiliation.*
> *(c) The action would be heard by the Federal Court or the FCFCOA.*
> *(d) The claimant would first need to make a complaint to the OAIC and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme.*
> *(e) Where the IC or an EDR is satisfied there is no reasonable likelihood that the complaint will be resolved by conciliation or the IC decides a complaint is*

[65] Proposal 23.6, p. 243, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[66] Submission by the Office of the Australian Information Commissioner dated 23 December 2021 on the discussion paper released by the AGD in October 2021, at pages 184-185.
[67] Proposal 26.1, p. 279, ibid

unsuitable for conciliation, the complainant would have the option to pursue the matter further in court.

(f) In cases where the IC has decided that a complaint is unsuitable for conciliation on the basis that the complaint does not involve an interference with privacy or is frivolous or vexatious, the complainant should be required to seek leave of the court to bring an application in the court.

(g) The OAIC would have the ability to appear as amicus curiae or to intervene in proceedings instituted under the Privacy Act, with leave of the court.

(h) Remedies available under this right would be any order the court sees fit, including any amount of damages.

Appropriate resources should be provided to the Courts to deal with these new functions."[68]

10.3. We do not consider that a direct right of action is justified. However, if this proposed reform is progressed, we support the proposal that claimants are to first make a complaint to the OAIC and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme as this will, at least to some extent, limit the number of matters that will come before the courts.

10.4. We also support the design principle that in cases where the Information Commissioner has decided that a complaint is unsuitable for conciliation on the basis that the complaint does not involve an interference with privacy or is frivolous or vexatious, the complainant should be required to seek leave of the court to bring an application in the court. This would help prevent a flood of claims that would consume the time and resources of the courts from other parties who have a substantial case involving a more serious case.

10.5. We also recommend a requirement that the claimant should also be obliged to participate in the conciliation process in good faith unless the claim is assessed as being unsuitable for conciliation on the basis that is does not involve interference with privacy or is frivolous or vexatious.

10.6. Overall, we remain concerned that the introduction of a direct right of action for individuals to litigate a claim for breach of their rights under the Act is still likely to lead to a large number of lawsuits which would further burden the court system and severely tie up and tax business resources when there may be other more appropriate means for individuals to seek redress.

The possibility of such lawsuits happening is not hypothetical and has already happened in the US in the context of the *California Consumer Privacy Act* (CCPA), which saw around 50 class-action lawsuits being filed under the CCPA's direct right of action in the short span of seven months since the CCPA went into effect on 1 January 2020.[69] This was despite the direct right of action being narrowly scoped in the CCPA.

10.7. Consequently, we reiterate our view that a direct right of action should not be introduced, and that any dispute or complaint about a breach of an individual's rights under the Act ought to be resolved through the existing avenues in the Act for conciliation, investigation and/or determination by the OAIC (collectively 'OAIC Resolution Process). This would also allow the OAIC to create a consistent body of regulatory advice for consumers and industry alike.

10.8. If a direct right of action were to be implemented, it ought to be restrictively crafted. In addition to the requirement to first make a complaint to the OAIC and the requirement to seek leave of the court where the IC finds that a complaint is unsuitable for conciliation, amongst other things:

[68] Design elements to Proposal 26.1 p. 279, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023

[69] Holland & Knight LLP, *Holland & Knight Alert: Litigating the CCPA in Court*, Jul 2020, https://www.hklaw.com/en/insights/publications/2020/07/litigating-the-ccpa-in-court

- the direct right of action should only be available in respect of any dispute or complaint about a serious interference with privacy, where:
    - the OAIC Resolution Process is exhausted or completed in respect of the dispute or complaint; AND
    - the OAIC has not dismissed the dispute or complaint; and
- there ought to be a reasonable maximum award limit for compensatory claims;
- a notice requirement and opportunity for the APP entity to address an alleged interference with privacy before steps are taken to initiate legal action;
- if a respondent wants to resist an application to the court for leave in relation to a direct cause of action, oral hearings should be avoided, and the respondent should not incur costs if the leave is granted; and
- there ought to be an effective deterrent against frivolous and vexatious disputes and complaints, such as the applicant being liable for costs on an indemnity (solicitor/client) basis.

10.9. We understand that the Report proposes a mid-tier penalty provision (at Proposal 25.1) to cover interferences with privacy without a serious element. However, despite this proposal, we encourage further consideration of a serious harm threshold to ensure disputes and complaints which are not sufficiently serious are not burdening the court's resources.

Statutory tort

10.10. The Report proposes to

> *"Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123. Consult with the states and territories on implementation to ensure a consistent national approach."*[70]

10.11. We observe from Chapter 26 of the Discussion Paper that the concern the AGD wishes to address, through the possible introduction of a tort, are breaches of privacy instigated by individuals against other individuals,[71] where there is currently no common law remedy available. Breaches of privacy instigated by individuals are largely outside the scope of a member organisation such as Communications Alliance, and therefore, we did not offer a view on which of the options presented in the Discussion Paper would best address this concern.

10.12. However, we remain concerned with the proposed introduction of a statutory tort, due to its potential to lead to many frivolous actions and predatory lawsuits which may burden the court system and corporations targeted by such lawsuits and do not believe there is sufficient evidence to warrant the introduction of a tort that would also capture entities already captured as APP entities under the Act.

10.13. If a statutory tort was to be introduced, we support a model that rests on sufficiently high thresholds, i.e., the tort must only be for serious invasions of privacy, and the invasion must have been committed intentionally or recklessly.

In that respect, we support the ALRC Report 123 model.

[70] Proposal 27.1, p. 287, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023
[71] p.191, Attorney-General's Department, *Privacy Act Review Discussion Paper,* October 2021, which summarises issues raised in submissions to the Issues Paper including intimate-image abuse and individuals accessing and using personal information about other individuals, for example for blackmail or in Family Court proceedings.

12. Notifiable data breaches scheme

10.14. In the event of an eligible data breach, APP entities will focus their attention and resources at managing and remediating the breach to minimise potential consumer harm. It may be well be possible that APP entities do not have substantial information to provide within 72 hours of becoming aware of an eligible data breach.

We understand that the Report refers to entities having the opportunity to provide subsequent updates when not all information is known within the first 72 hours. Nonetheless, we see the new requirement as inefficient given the existing threshold (as soon as practicable) allows for full and accurate information to be provided in the first instance.

10.15. However, we support the proposal at 28.2 that entities be required to take reasonable steps to implement practices, procedures and systems to enable it to respond to a data breach.

10.16. In line with other observations, we nota that the controller-processor distinction ought also to be applied to eligible notifiable breaches.

If a data breach is notifiable to either the IC or persons affected by the data breach, this should be limited to the controller of the data making the notification. Processors should advise the controller if they become aware of data breach. If the processor were to notify persons affected by the data breach without the controller's input, this may undermine the position of the controller and cause unnecessary confusion.

13. Making of Industry Codes

11.1. The Report, proposes the following amendment in relation to the making of APP codes:

"Amend the Act to give power to the Information Commissioner to make an APP code where the AttorneyGeneral [sic] has directed or approved that a code should be made:

- *where it is in the public interest for a code to be developed, and*
- *where there is unlikely to be an appropriate industry representative to develop the code.*

In developing an APP code, the Information Commissioner would:

- *Be required to make the APP Code available for public consultation for at least 40 days,*
- *Be able to consult any person he or she considers appropriate and to consider the matters specified in any relevant guidelines at any state in the code development process."*[72]

(We assume that the proposal would be implemented through an amendment of section 26G of the Act.)

11.2. The Report proposes that explanatory materials to the amending provisions should provide additional detail as to when the second limb (unlikeliness of an industry representative to develop a code) would be likely to apply.

11.3. We are not convinced that there are circumstances where it is unlikely that an appropriate industry representative to develop an APP code can be identified, and we would welcome more clarity as to the factors that would be applied in determining whether such an unlikeliness existed.

[72] Proposal 5.1, p. 48, Attorney-General's Department, *Privacy Act Review Report 2022*, February. 2023

11.4. If in such circumstances the IC indeed is given the delegated power to make APP codes, it is imperative that these codes, as proposed in the Report, are subject to disallowance by Parliament.

11.5. In circumstances where an APP code is being developed by the IC, Proposal 5.1 suggests a mandatory consultation period of 40 days, instead of the currently mandated 28 days for codes developed through industry representatives.

We urge the AGD to extend this period to 60 days, given industry is no longer the code developer and will, therefore, not be as familiar with the draft code as under the industry-led model. An extension of only 12 days does not sufficiently account for this. It is also appropriate given the likelihood that a code will be applicable economy-wide or at least to a broad sub-set of the economy.

Given the complexity of privacy law, especially as it finds its application against an increasingly technological background that even many 'tech-minded' people find 'mind-boggling' (consider, for example, artificial intelligence and the recent discussions triggered by ChatGPT), consumers and community representatives also require a longer period to adequately reflect on the draft codes.

It should also be noted that the ever-increasing number of consultation processes on various topics over the past years means that, irrespective of any change in approach, the legislative consultation periods (typically 28 days) have simply become inappropriate over time and ought to be adjusted accordingly to allow stakeholders to participate in the many processes that often run in parallel. (For reference, with the same number of staff, Communications Alliance has made around 15-20 submissions in 2010 but made 66 submissions in the FY2021/22 and only slightly less in the following year due to Parliament being prorogued for federal elections.)

11.6. Importantly, the proposal only includes the possibility for the IC to consult with any person, including industry, at any stage in the development of the code and the matters specified in the relevant guideline – which the IC her/himself develops.

This mere optionality does not provide sufficient safeguards that industry will indeed be appropriately involved in the development of the APP codes. Instead, the legislation, if amended accordingly, ought to mandate that the IC consult with the relevant industry section(s) at the beginning of the process to map out a framework for the development of the code, including the timeframes, and at several juncture points in the development process. Such a process would reflect current practice where codes are developed by industry in the telecommunications sector for registration by the regulator, the Australian Communications and Media Authority (ACMA).

Temporary APP codes

11.7. The Report proposes at Proposal 5.2 to

"*Amend the Act to enable the Information Commissioner to issue a temporary APP code for a maximum 12-month period on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.*"

11.8. The Report provides an example of when such a power might be used stating "*the IC should have power to develop a temporary urgent code to enable an APP code to be made more quickly to respond to an urgent situation such as during a pandemic.*"

11.9. However, Emergency Declarations are currently available, and the Report proposes at Proposal 5.4 to "Ensure the Emergency Declarations are able to be made in relation to ongoing emergencies". The Report again uses the example of a pandemic for when this might be appropriate, and we support this proposal.

11.10. To the extent that powers are required for emergency sharing of information, this is already captured under Proposal 5.4 so it is not clear what scenario would need an

urgent temporary code such as proposed in Proposal 5.2. In this context, we cannot see a justification for such broad unilateral powers to be conferred on the IC, and we thus do not support Proposal 5.2.

14. Implementation timeframes

12.1. We note that some of the changes contemplated in the Report may have substantial implications for APP entities and urge the Government to ensure that any such changes are accompanied by significant implementation timeframes for entities.

Such implementation timeframes should be developed after consultation with APP entities and ought to be enshrined (e.g., via commencement dates) in the legislation.

12.2. In order to facilitate a practical implementation regime, we recommend the introduction of the revised Act in tranches with sufficiently staggered commencement dates and, where clarification of specific proposals has been referred to additional guidance, codes or other checklists these be finalised prior to relevant implementation periods.

15. Other observations

12.3. As the Report's proposals are further developed, it is critical that there is adequate consultation and coordination across Government on related legislative and policy work programs relating to areas such as cyber security and online safety. This is due to the inter-dependencies of these areas, which is acknowledged in the Report. For example, Section 21 of the Report which addresses security, retention and destruction indicates a need to draw on technical advice from the Australian Cyber Security Centre. Separate proposals relating to children's safety refer to the need to consult with the Office of the eSafety Commissioner. The Department of Industry, Science and Resources also is separately considering how regulatory settings and systems can maximise the opportunities of AI and automated decision-making.

12.4. There is some tension between the work programs noted above, and they must be considered and developed in a coordinated manner to avoid inconsistencies. For example, the Office of the eSafety Commissioner requested the development of industry codes on the basis of a Position Paper outlining detailed positions around online safety and measures by online services to identify potentially harmful content and to protect end-users. The implementation of these measures often requires personal information and/or de-identified information. On the other hand, the collective objective of the proposals in the Report is the protection of an individual's personal information, including through limiting the collection, use and disclosure of personal information to what is directly relevant and necessary to accomplish a specified purpose. These tensions must be resolved to ensure both individuals and APP entities have certainty and trust in how personal information will be handled.

12.5. We highlight that the review of the Act also ought to take into consideration other reform processes and pieces of legislation that have the potential to impact on the proposed reform of the Act, for example the Electronic Surveillance Reform which proposes a new definition of 'communications' which in turn are subject to a number of privacy and non-disclosure requirements under Part 13 of the *Telecommunications Act 1997*.

12.6. Consequently, for the development of any further Guidelines, checklists, codes or other instruments, it is important that these are developed in close consultation with industry and prior to any implementation period commencing.

16. Conclusion

Communications Alliance looks forward to continued engagement with the AGD and other relevant stakeholders on ensuring that all Australians' privacy continues to be adequately protected.

We continue to lend our support to the overarching objectives of the Privacy Act Review and stand ready to work with Government to facilitate an effective and efficient adoption of a new, privacy regime that is fit for the digital age, limits friction of cross-border dealings, adequately protects individual's privacy and gives individuals appropriate control over their data while striking an appropriate balance of the various interests involved in today's data societies.

For any questions relating to this submission please contact Christiane Gillespie-Jones on 02 9959 9118 or at c.gillespiejones@commsalliance.com.au.

Published by:
COMMUNICATIONS ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E
info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507