COMMUNICATIONS
ALLIANCE LTD

Communications Alliance Submission

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

Privacy Act Review Discussion Paper

28 January 2022

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.

1. Introduction

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

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

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* (Privacy 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 Privacy Act with leading data privacy and data protection statutes in other jurisdictions.

Many entities regulated under Australian data privacy laws already conduct operations in multiple jurisdictions or have ambitions to do so.

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.

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.

Particular care needs to be taken to ensure that the law 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. Getting this balance right requires careful consideration of the interaction of different requirements and prohibitions, and associated limitations and exceptions, that together make up the data privacy statute.

One key difficulty in commenting on the Discussion Paper is that it puts forward a menu card of possible reforms, many of which cannot be properly commented on without understanding how a proposal would operate within the context of a complete statutory

package. There is, therefore, a substantial risk that comments received by the AGD in response to particular proposals in the Discussion Paper that are context-dependent may be misinterpreted or misapplied. In this regard, we clarify that many of our comments are context-specific and should be viewed in the context of a complete statutory package.

It might be erroneously believed that any problems that arise through context dependency could be addressed by broad requirements that are fine-tuned through active exercise of discretions by a Minister or regulator. However, it is not appropriate to enact a manifestly over-inclusive statute and provide the regulator (or the Minister) with discretions to make instruments which limit elements of over-inclusiveness. Besides problems of uncertainty that over-extensive regulation creates, it delays and/or stifles innovation. It also, perversely, discriminates against smaller businesses, which may not have the necessary resources to manage and ensure regulatory compliance, resulting in greater regulatory risk for such businesses.

Accordingly, we urge consideration by AGD of the combined and cumulative effect of proposals for reforms, and to note the need to describe a complete package as an interworking whole for further industry consultation, before commencing legislative drafting. We particularly urge caution in relation to advocacy of elements of the European Union's General Data Protection Regulation (EU GDPR) without also proposing corresponding or other otherwise analogous limitations and exceptions as apply under EU GDPR.

2. Intersection with the Online Privacy Bill

2.1. The reform of the Privacy Act is being progressed in parallel to other significant proposed reform processes, most notably the exposure draft of the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (Bill) which has been released for public consultation in October 2021 (consultations closed on 6 December). Part of the Bill's contents are currently subject of the ongoing inquiry of the House Select Committee on Social Media and Online Safety.

2.2. The draft Bill specifically targets social media and large online platforms. As highlighted in our submission in response to the exposure draft of the Bill, neither the Consultation Paper that accompanies the exposure draft, nor the Regulation Impact Statement offer convincing evidence as to the validity of the claim around the particular privacy challenges posed by social media and online platforms in relation to compliance with the Australian Privacy Principles (APPs) and the need for urgent regulatory intervention.

2.3. While the Bill describes the measures that are to be contained in a future code, it already sets a prescriptive framework pre-empting, or forcing industry to pre-empt, substantial areas of reform that are still being discussed in the separate process of the Privacy Act Review and are already highlighted as being controversial in the Discussion Paper. Those areas include, for example, the definition of 'personal information', requirements for valid 'consent', circumstances in which express consent must be sought and obtained, the scope of operation of transparency requirements in relation to respectively privacy policies and privacy (collection) notices (vs what must be addressed in each), the extent to which use of technical information for differentiated treatment of users will be regulated under the Privacy Act, whether there should be a broad form opt-out option for users of online services, and reasonable bases for exceptions from an opt-out option (i.e., any carve-down for reasonably anticipated or compatible uses or legitimate uses or interests.

2.4. Consequently, given the lack of evidence that urgent measures are required for social media service and large online platforms and why those have been singled out for a separate reform process, we believe that consideration of the matters contemplated in the Bill, if required at all in this form, ought to be delayed until the Privacy Act Review process (and also the Age Verification Roadmap process) has sufficiently progressed.

3. Objects of the Act

3.1. The Discussion Paper proposes to amend the objects in section 2A of the Act, including introducing the concept of public interest. It is suggested to amend section 2A(b) as follows: [amendment highlighted in ***bold***]

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

3.2. As we have previously noted, the current Act appropriately emphasises the need to balance the protection of the privacy of personal information against the interests of entities when carrying out their functions and activities.

It is, indeed, these activities that brought about many of the services and attributes that consumers value or even take for granted. It is, therefore, not appropriate to cast the right to privacy of individuals and legitimate commercial needs to use personal information as irreconcilable and incompatible positions that are, by default, at odds with each other.

Bearing the proposed additional public interest test in mind; at what point would one consider that an activity or function moves from the realm of the entity's interest into the public's interest? And who makes this determination? Is this, for example, when some benefit is delivered, although it is not apparent to the average individual, as may be the case with a security or fraud-prevention feature? Or, rather, when a certain percentage of individuals finds a service or feature useful? And what percentage would that be?

3.3. The above illustrates that the inclusion of public interest in object is inappropriate as it is impractical in its application, as it may be difficult for entities to demonstrate the public interest benefit, although it may well exist, either immediately or in the future.

Consequently, we reiterate our belief that the two interests – the protection of privacy of personal information and business interests – are both legitimate and, importantly, both provide benefits to individuals and society at large, through the protection of personal information on the one hand and enhanced and expanded product and service offerings on the other.

Adding a concept of public interest introduces substantial uncertainty to evaluation and application of this balance.

An alternative approach would be to recognise that there is both an individual interest, and a societal interest, in protection of privacy of individuals, and that both this individual interest, and the collective (societal) interest, should be considered in applying the first limb of the balancing factors.

In any event, introduction of an unclear and uncertain qualifier to the second limb (legitimate commercial interest) of the balancing factors risks stymying innovation and investment in key areas of the economy.

Consequently, we reject the proposed amendment of section 2A(b).

In any event, the concept of 'activities undertaken in the public interest' is highly normative and uncertain. If the legislature's aim is to signal that furtherance of interests of entities in carrying out their functions or activities should be qualified by consideration of possible societal detriment, a more appropriate formulation might be interests of entities in carrying out their functions or activities to the extent that those functions and activities are not inconsistent with benefit to Australian society. This would also ensure that entities that have commercial interests that neither further societal benefits (at least not currently foreseeable benefits, noting that many benefits of innovations only been realised over time) nor have detrimental effects, are permissible within the general protection parameters.

3.4. We also highlight, including against the background of harmonisation of privacy frameworks where appropriate and possible, that the EU GDPR expressly recognises legitimate interests as one of the lawful bases for the processing of personal data by data controllers and third parties to balance the interests of individuals and businesses with the right for transparency and privacy of individuals.

Legitimate interests include processing for purposes of preventing fraud, ensuring network and information security, and developing products and services to better meet customer needs, among others. As enumerating the range of these legitimate interests in statutory language is impractical, the legitimate interest basis provides companies the flexibility to process personal data for these purposes, while ensuring that the interests of individuals are appropriately protected.

Having a broader legitimate interests exemption reduces the likelihood of consumers receiving repeated notifications for essentially the same processing activity or requests for activities which only have a minimal impact on their privacy. This also encourages entities to adopt a risk-based approach to handling personal data, instead of over-relying on the 'notice and consent' model.

Therefore, we recommend recognising legitimate interests as a lawful basis for the processing of personal information, alongside requirements of fairness and reasonableness.

4. Definition of 'personal information'

Expanded definition of personal information

4.1. The Discussion Paper proposes a change to the definition of personal information. The proposed new definition reads:

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.

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

4.2. The Discussion Paper indicates that submissions largely supported an amendment of the definition of personal information to more explicitly capture technical information on the basis of concerns around identity theft and other harms in relation to increased use of data.[1]

4.3. However, we question whether the proposed change of definition would result in significant improvements in relation to identity theft or any other cybersecurity-related harms associated with the misuse of technical information that would now be captured under the definition of personal information as a result of the change.

4.4. We also note that the purported clarification, "An individual is 'reasonably identifiable' if they are capable of being identified, directly or indirectly," does not appear to explain when an individual is 'reasonably identifiable', given that the clarification uses an absolute, i.e., 'capable', to describe the state of 'reasonably identifiable'. If the absolute standard of 'capable' is being applied, then a limiting threshold of 'reasonably' ought not be used in the same sentence, or at least not unless other factors are included to delineate capability of identification from other tests, such as a remote or hypothetical risk of identification.

[1] p. 22, Attorney-General's Department, *Privacy Act Review Discussion Paper*, Oct. 2021

4.5. Moreover, we continue to believe that the current definition, together with the guidance[2] released by the Office of the Australian Information Commissioner (OAIC) following the case of Privacy Commissioner v Telstra Corporation Ltd (Grubb Case), provides sufficient clarity with regard to the definition of personal information, including the matters discussed in the Grubb Case. To the extent the current definition and OAIC guidance requires further clarification, we suggest that additional guidance be provided. Such guidance would also be able to be updated more flexibly as technology evolves, to ensure that new types or applications of technical information are covered.

4.6. If the definition of personal information were to be amended, an overly broad definition that does not consider context should be avoided, particularly in relation to information which is not collected, used, or disclosed in a way that materially impacts an individual's privacy, and which could comprise commercially sensitive business secrets**.**

4.7. In particular, we caution against a broad inclusion of technical and online identifiers as contemplated in the Discussion Paper. While it may be true that the current status of communications data (so-called metadata) could benefit from additional clarification through guidance, so far, we have not seen evidence that the inclusion of the data would actually provide consumer benefit. In particular, metadata may be used to differentiate between individuals without facilitating or enabling or otherwise carrying risk that those individuals may be or become reasonably identifiable. This differentiation may improve consumer welfare – for example, by enabling presentation of material or results inferred to be more likely of interest to a particular (unidentified) transactor, or detrimental to consumer welfare, such as where there is illegal discrimination between (unidentified) transactors. Consumer protection laws and regulation is the most appropriate tool to address such issues of consumer welfare. Metadata that is reasonably likely to be used to identify individuals is already captured as indirect identifiers, as stated in the OAIC guidance applying the reasoning of the Full Federal Court in the Grubb Case. We caution that a change to capture a wider range of identifiers in the definition of personal information would impose substantial costs on industry, which are likely to be passed on to consumers and may stifle innovation or prevent new technologies and services from being deployed in Australia.

4.8. There is considerable confusion in current discussions between stakeholders in these reforms as to the purpose, and therefore the utility, of (1) listing of types of information capable of being covered by the definition of personal information, and (2) inclusion of references to technical data associated with a transaction or transactor, such as a device identifier or online tracking code, as identifiers or pseudo-identifiers.

4.9. Often this confusion arises because a relevant type of information and/or a pseudo-identifier depends upon context. As noted above, the relevant question is, whether it is reasonably practicable for a particular entity to associate the information in question with an identifiable individual taking into account the nature of the information, whether the data environment in which that information is held and managed, and the availability or otherwise in that data environment of other potentially identifying information. The assessment involves consideration of the particular circumstances of that entity and that entity's reasonable access to other information, the nature of the relevant information, and the data situation in which that relevant information is collected and handled.

4.10. These contextual factors or considerations might be referred to in the Act.

4.11. By contrast, listing types of information, and/or technical codes or other pseudo-identifiers, may promote confusion, because the contextual evaluation is still required

[2] As accessed on 26 Nov 2020: https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/

to determine whether particular types of information and/or technical codes are in fact identifying in a particular context.

4.12. 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 identified 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 infer 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. 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 not personal information.

4.13. 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 (sometimes called a "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 deidentified, or effectively anonymised, 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).I Information within these other data environments would be personal information.

4.14. 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.

4.15. There is significant risk that over-expansive and prescriptive coverage in the Privacy Act of technical data and other pseudo-identifiers, and of data handling within data environments in which information is effectively isolated and anonymized, would reduce regulatory incentives for entities to establish and operate appropriately controlled and safeguarded environments for conduct of data analytics, and to substitute direct or indirect identifiers with other information (e.g., transaction or transactor codes), which effectively preclude identification or reidentification of individuals.

4.16. Much of the technical information that participants in the telecommunications network services sector hold (and produce in the course of their normal network operations) should not be considered personal information unless it is linked (e.g., via account details) to a specific individual. Over-expansive and prescriptive coverage in the Privacy Act of technical data and other pseudo-identifiers would have significant consequences for the business-as-usual activities and operational requirements of telecommunications providers. An expansive definition of personal information,

coupled with the lack of appropriate exceptions/bases for the handling of personal information, would lead to difficulties in being able to use a wide range of information currently required for the operation and protection of telecommunications networks, such as information required for, among other things:

- telecommunications networks to interoperate and properly convey telecommunications traffic;
- network assurance activities such as fault finding, capacity planning and optimising network performance;
- fraud and cybercrime prevention and investigation activities; and
- national security and law enforcement investigations.

These uses should not require transparency to affected individuals, as would otherwise be required if the definition of personal information were extended as canvassed in the Discussion Paper. Indeed, over-expansive and prescriptive transparency actually decreases the value of transparency as to acts or practices reasonably likely to cause privacy harms to individuals, by increasing information overload and notice fatigue.

4.17. In this context, we again note that much of the technical information that our industry holds (and indeed produces through their normal network operations) should not be considered personal information.

Inclusion of a non-exhaustive list of potential types of 'personal information'

4.18. The Discussion Paper proposes to include a non-exhaustive list of types of information capable of being covered by the definition of personal information.

4.19. We oppose this suggestion as it risks diluting the circumstantial and contextual approach to the definition that we believe is essential. Such listings are also unlikely to withstand the rapid dynamic evolution of technical data and online identifiers and risk becoming outdated relatively quickly. Moreover, such listings also bear the risk of creating confusion among consumers who may believe that the listed types always constitute personal information.

4.20. Instead, the Act could state the principles and outcomes desired to be achieved in respect of information as it may constitute personal information. The OAIC could then supplement these outcomes with appropriate guidance which can be amended as technological change may demand.

4.21. If a list were included, it should be made clear that the information on the list is only capable of being covered by the definition of personal information, but that it will depend on the context as to whether the information actually constitutes personal information. Furthermore, it would also be helpful to include a list of data that is explicitly excluded from the definition of personal information. For example, location information could constitute personal information in the case of precise geo-location data (i.e., longitude and latitude data; especially when combined with other information). Mobile cell tower location information, however, would be less likely to constitute personal information. Similarly, a static IP address that clearly identifies a source (user) could be considered personal information, whereas a dynamic IP address (in a network which uses Carrier Grade NAT technology) which may attach to hundreds of users at a specific point in time might not be personal information etc.

Expansion of definition of 'collection' to include inferred or generated information

4.22. The Discussion Paper proposes to amend the definition of 'collection' "to expressly cover information obtained from any source and by any means, including inferred or generated information."[3]

4.23. Inferred or generated information includes information that is usually not generated by or on behalf of the individual to whom it pertains, but instead comes into existence through derivation or inference by another party or individual, or indeed a machine-based process.

4.24. Often, entities have made substantial resource investments into data analytics and processes that generate the inferred data. The inferred data may or may not be identifiable, but is valuable confidential intellectual property of the entity, without which it would not have come into existence, and which provided a value-add that often finds application further downstream in features and services which, in turn, enrich a user experience or enhance a service.

4.25. The Consumer Data Right appropriately recognised the conflict of the right to access certain consumer data versus intellectual property rights and excluded 'materially enhanced data', i.e., data that is significantly more valuable than the source data because of the application of fresh insight or analysis.

Similarly, it may not be appropriate to grant individuals access to all inferred or generated data as such access may reveal commercially sensitive information or trade secrets about how the inferred data has been generated or obtained.

4.26. It is also important to note that the proposed amendment would trigger the attendant notification obligations each time new information is inferred or generated. Such notifications would not only be confusing but almost certainly lead to 'notification fatigue', similar to the fatigue experienced in response to the 'cookies notices' that entities are required to provide in response to the EU ePrivacy Directive.

4.27. Consequently, we believe that inferred and generated information ought not be expressly covered in the definition of 'collection', or at least substantial caveats would need to be introduced to address the concerns raised above. Such information also ought not be subject to all notice and consent requirements of personal information.

Information to be anonymous to fall outside the scope of the Act

4.28. The Discussion Paper proposes to amend the Act to require information to be 'anonymous' rather than 'de-identified' for the Act to no longer apply. The Discussion Paper proposes that information would be considered anonymous if the risk of re-identification is 'extremely remote or hypothetical'. [4]

4.29. The Discussion Paper notes the various submissions that have raised concerns that this would mandate an unworkably high standard, but simply asserts the contrary, without providing further evidence as to why this would not be the case.

4.30. The standard of anonymisation is too high – even more so if an expansion of personal information to include technical data is being contemplated. The destruction or anonymisation of technical information, such as communications metadata, which is not retained or used in a way that an individual would be identified in the ordinary cause of operations would create unnecessary or even unsurmountable compliance burdens for the industry with little or no discernible privacy benefit for consumers.

4.31. Consequently, we believe that the current standard of de-identification ought to be retained.

[3] p. 28, Attorney-General's Department, *Privacy Act Review Discussion Paper*, Oct. 2021
[4] pp. 30/31, Attorney-General's Department, *Privacy Act Review Discussion Paper*, Oct. 2021

4.32. If anonymisation were to be introduced as a new standard, then it ought to be clarified that the test for anonymisation is a relative one, i.e. the test of whether data can be considered anonymous is relative to the means available to the data controller at the time (note our comments on a data controller/processor distinction further below), as currently also contemplated in the UK.[5] The UK Government concluded that this approach would give "organisations more confidence to anonymise data and use it more innovatively within their own organisations."[6]

4.33. It is critically important to get right how the privacy statute addresses de-identification, across the spectrum from pseudonymisation to full anonymisation. Many societally beneficial applications of data relating to citizens depend upon use of controlled and safeguarded data analytics environments within which individual level (transaction and transactor) data may be linked and analysed with appropriate assurance of privacy and security by default and design, both for the handling of data isolated within the controlled data environment, and outputs released from those controls.

4.34. If an entity demonstrably (reliably and verifiably) disables itself from capability to associate online data with an individual through technical means (i.e., through masking, anonymity, differential privacy, privacy-preserving machine learning and synthetic data, as well as through data transformations such as aggregation) and environmental (operational, contractual and other) conditions (controls, safeguards and guardrails), such that individuals are not identifiable by any means reasonably likely to be used (i.e., the risk of harm to an individual of identification is sufficiently remote), the information is and should remain regarded as effectively or functionally anonymised (deidentified) and not be regulated as personal information.

4.35. It is not possible in practice to ensure that most consumer data is anonymised to the point where re-identification can be assured to be impossible over time: other data sources may become available that facilitate patter or mosaic identification attacks, or technical processes for identification attacks may involve, in ways that cannot reasonably be anticipated by a regulated entity. For this reason, state of the art analyses of anonymisation technologies and techniques draw a distinction between 'functional anonymisation' (also sometimes called 'effective anonymisation'), and 'complete anonymisation' (also sometimes called 'full anonymisation') (viz., anonymisation assured as pervasively reliable over time). Many experts consider that complete (full) anonymisation is not possible in practice for most consumer data.

4.36. If 'anonymisation' is to replace 'de-identification' as the relevant statutory term, it needs to be clear:

1 that the standard remains 'functional [effective] anonymisation', where individuals are not identifiable by any means reasonably likely to be used – i.e., the risk of reidentification is sufficiently remote; as compared to full anonymisation (where individuals cannot be identified by any conceivable means);

2 what is the standard for assessment of residual (after implementation of mitigations) reidentification risk? The appropriate standard is 'very low' or 'sufficiently remote'. The appropriate standard is not (as the Discussion Paper suggests) 'extremely remote or hypothetical', which appears to equate to complete (full) anonymisation, which does not reflect state of the art analyses of technologies and techniques for reasonably practicable anonymisation.

[5] p. 46, para. 123, Department for Digital, Culture, Media & Sport (UK, Data: A new direction, Sept. 2021
[6] ibid

Expansion of sensitive information

4.37. The Discussion Paper proposes to expand the categories of sensitive information to include, among other additional information, location data, on the basis that such information can be of an intrusive nature.[7]

4.38. We do not support such an expansion, on the basis that the potential benefits do not outweigh the attendant costs/detriments. Importantly, we reiterate that location information in general might only become sensitive information in limited circumstances.

4.39. Amending the definition of sensitive information may also result in additional notifications being sent (by organisations erring on the side of caution) thereby increasing the risk of notice and consent fatigue.

4.40. Further, an expanded definition is also likely to impact the delivery of services or products with no clear privacy benefit. For example, mobile location data that is collected in network transactions to ensure the network is ready to send a call to the right cluster of mobile cells when a call is received by the network, is not inherently sensitive. However, inclusion of location data in the definition of sensitive information may have the effect of requiring network operators to obtain consent from an individual to collect and use that information for purposes that present no material privacy impact.

4.41. If the categories of sensitive information were to be expanded, it would be critical to ensure that the additional data categories are clearly defined. For example, the term 'location data' as such (as compared with 'geolocation data') does not provide sufficient clarity for entities as to which types of location data with varying degrees of geographic accuracy or dependency on other data sources would be included in the category.

5. Controller / Processor distinction

5.1. As noted in our submission to the Issue Paper, we believe that the revised Act would be improved by incorporating a data controller/processor distinction to clearly allocate responsibilities pertaining to notification, consent, erasure and security (including destruction and de-identification) of personal information to the entity that is best placed to handle those, i.e. usually the controller. A controller/processor distinction would not only assist with minimising duplication of effort for businesses (complying with obligations) and individuals (dealing with duplicative notices and requests for consent), but would also facilitate administration of the Privacy Act by the OAIC, ultimately enhancing transparency and certainty of implementation for all participants of the regime.

5.2. Importantly, as recognised in the Discussion Paper, such a distinction would also align Australia's privacy regime with the regimes many other jurisdictions, including jurisdictions like Canada and India which are looking to revise or adopt personal information protection laws that incorporate a controller/processor distinction.[8].

5.3. Indeed, given the increasing complexities of data flows in our digital economies, it is hard to see how modern privacy laws would be able to function appropriately without such a distinction and, consequently, we urge the Department to incorporate this important distinction into the Act, despite the additional complications that this may trigger with regards to the currently existing small business exemption (refer to our comments below).

[7] pp. 33/34, Attorney-General's Department, *Privacy Act Review Discussion Paper*, Oct. 2021

[8] pp. 157/158, ibid

5.4. We note that careful consideration should be taken to ensure inherent gaps in the GDPR (e.g. controller-controller relationships), are being addressed. Extensive OAIC guidance is required. However, the fact that an incorporation of a controller/processor distinction into Australian privacy law may require careful preparation (also with respect to potential exemptions, see below) must not mean that it should not be attempted or be put into the 'too hard basket'.

Small business exemption

5.5. We do not support the removal of the small business exemption. However, as noted above, we also do not believe that the existence of the exemption gives sufficient grounds to not proceed with a controller/processor distinction in Australian privacy law.

5.6. Further discussions dedicated to this topic ought to be scheduled (and be allowed sufficient time) once other issues have been settled in principle.

6. Making of Industry Codes

6.1. The Discussion Paper, at proposal 3.1, canvasses an amendment to the Privacy Act, to allow the Commissioner to make an APP code on the direction or approval of the Attorney-General:

- where it is in the public interest to do so without first having to seek an industry code developer, and
- where there is unlikely to be an appropriate industry representative to develop the code.

6.2. Section 26C(3)(a) as now in force provides that an APP code may impose additional requirements to those imposed by one or more of the APPs, so long as the additional requirements are not contrary to, or inconsistent with, those principles.

6.3. Section 26G (Development of APP codes by the Commissioner) provides a limited control as to the Commissioner using code-making authority to expand coverage and requirements of the privacy statute. The Commissioner may develop a code if (1) he/she is satisfied that to do so is in public interest, and then only if (2) the Commissioner has requested (under subsection 26E(2)) a code developer to develop a code and the request has not been complied with, or the request has been complied with but the Commissioner has decided not to register, under section 26H, the APP code that was developed upon request.

6.4. A key current control over over-expansive coverage of codes is that codes are developed through consultations within an industry sector led by an industry code developer, and not imposed upon an industry sector by unilateral action by the Commissioner.

6.5. This control is appropriate, regardless of whether or not that unilateral action is directed or approved by the Attorney-General. If the Commissioner was empowered to make an APP code of its own volition and on the Attorney-General's view of 'public interest', that code could add new requirements to those imposed by one or more of the APPs and otherwise impose substantial additional regulatory burdens upon APP entities. This would be an inappropriate delegation of quasi-legislative authority to the Commissioner. The Commissioner would be effectively unregulated by the Parliament, acting at the discretion of a Minister exercising that Minister's personal and political view as to the public interest.

6.6. The Commissioner's power to step in to determine a code should be a qualified reserve power, only exercisable where an industry code developer fails to develop a code

after that industry code developer has been afforded a reasonable opportunity, and a reasonable timeframe, to do so.

6.7. As is clear from existing section 26C(3)(a), an APP code may impose additional requirements to those imposed by one or more of the APPs, limited only by the requirement that additional requirements are not contrary to, or inconsistent with, those principles. It would be an inappropriate delegation of quasi-legislative authority to the Commissioner to enable this discretion to be exercised by the Commissioner, unless:

- **an industry sector has been afforded a reasonable opportunity, and a reasonable timeframe, to address a request by the Commissioner for the industry sector to develop a code, and**
- **the relevant request states the nature of the additional requirements which the Commissioner requests that industry sector to address in a code and why the Commissioner considers those additional requirements to be in the public interest, such that the industry sector can be reasonably considered to be on notice as to the Commissioner's expectations and grounds for those expectations.**

6.8. A period of twelve months should be specified as a minimum period. Given the potential for the Commissioner to develop a code if an industry sector does not develop a code, we consider it most unlikely that the industry sector would fail to nominate an appropriate industry representative to develop a code.

7. Additional protections for collection, use and disclosure of personal information

7.1. The Discussion Paper at proposal 10.1 canvasses an amendment to the Privacy Act, to the effect that a collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.

7.2. We consider that adding a 'fair and reasonable' test is not appropriate. The test would introduce substantial uncertainty into data privacy governance, compliance and data risk assurance processes of regulated entities.

7.3. 'Reasonableness' as an over-arching, positive legal requirement is highly subjective – which is one reason why it has not become a standard adopted into Australian consumer protection statutes.

7.4. If the element of 'reasonable proportionality' is not considered to be sufficiently clearly stated as an element that regulated entities must apply when evaluating whether a collection is 'reasonably necessary' to achieve a stated purpose, this 'reasonable proportionality' could be added.

7.5. The Act already requires fairness as to the means of collection of personal information (per APP 3.5), which is an appropriate and sufficient control as to excessive or intrusive data collection practices.

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

8.1. The Discussion Paper at proposal 16.1 canvasses amendments to the Privacy Act, building upon a right to object (as discussed at Chapter 14), which would include an unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing.

An individual could still request to not receive direct marketing communications from an organisation.

If an organisation provides marketing materials to an individual, it should notify the individual of their right to object in relation to each marketing product provided. On receiving notice of an objection, an entity would be required to stop collecting, using or disclosing the individual's personal information for the purpose of direct marketing and must inform the individual of the consequences of the objection.

8.2. Many of our members do not collect personal information for the purpose of direct marketing, and only collect such information for the purpose of supplying telecommunications goods and services. Given such information is normally collected once and then used for multiple purposes, we struggle to understand how an objection could operate in this context, unless it is nothing more than the ability to opt-out of marketing, in which case, why introduce the right to object when people can simply opt out of direct marketing under existing regulatory frameworks? Hence, introducing a 'right to object' does not to add further value.

8.3. Furthermore, the Discussion Paper does not appear to distinguish between an entity that engages in direct marketing and an entity (e.g., a carriage service provider) that facilitates a direct marketing communication. It would not make any sense for the right to object to be exercised against the carriage service provider, which is simply carrying out another entity's instructions – which again highlights the importance of there being a controller/processor distinction in the Privacy Act, and for the right to object to be exercisable only against controllers.

8.4. Consequently, we consider that the opt-out election is too broadly stated to be reasonable and practical. To the extent that the legislature considers that it is appropriate for the Australian Privacy Act to afford affected individuals a right of election to opt-out from collection, or from particular uses or disclosures, of personal information about them, that right should:

- **be created through, and specified in, legislated settings, and not through exercise of discretion by the regulator;**
- **relate specifically to, and be separately exercisable in relation to, uses and disclosure of personal information for the purpose of targeted online advertising and other forms of direct marketing based upon differentiation between individuals;**
- **only be available only in respect of personal information that is being processed on the ground of consent (and not on any other ground, e.g., one of the permitted general conditions in section 16A of the Privacy Act);**
- **not be mandated where particular forms of targeting are inherent to and a reasonable incident of tangible benefits offered to individuals (i.e., as a quid pro quo for rewards or other consumer benefits provided by loyalty programs, or provision of services without payment of service fees);**
- **to the extent mandated for (or voluntarily offered in relation to) any context other than targeted online advertising and other forms of direct marketing based upon differentiation between individuals, be separated from the opt-out for targeting and direct marketing. The right should then only exercisable where those other uses and disclosures are not a reasonable incident of provision of a product or service. Where uses and disclosures are a reasonable incident of provision of a product or service, an affected individual can elect to not acquire or otherwise use the product or service;**
- **not include audience segmentation-based marketing where:**
  - **the factors (i.e., inferred interests or preferences or other characteristics) used to define the audience segment used for delivery of content are not created through use of personally identifying information;**
  - **there is no disclosure of personally identifying information; and**

- **relevant factors are not added to profile information about an identifiable individual.**

8.5. We reiterate that a controller/processor distinction ought to be adopted, and that the right to object ought to apply only to controllers.

9. Overseas data flows and extraterritorial application of the Act

Overseas data flows

9.1. We remain open to discussions around efforts that would move the Australian regime closer towards adequacy with respect to the EU GDPR, while simultaneously ensuring that the Australian privacy regime is tailored to Australia's legislative, cultural and business landscapes. Striking a good balance between international alignment and a focus on Australia's specific circumstances would likely lead to innovation to remain in Australia, strengthen Australian data-based export activities and make it easier for customers and service providers to communicate with each other with less reliance on other mechanisms, such as binding corporate rules or standard contractual clauses.

9.2. Our globally operating members would like to see a more defined scope of when entities can (or cannot) transfer personal information overseas. The current 'accountability' language in Australia's Act is very broad, and can lead to disputes between cloud service providers acting as data processors and customers in Australia as to what measures the cloud service provider is required to put in place to protect the personal data in question.

9.3. **Consequently, the proposal to have a mechanism of prescribing countries and certification schemes that provide substantially similar protections to the APPs appear useful and we would welcome this approach.**

9.4. **We also support the introduction of standard contractual clauses as proposed in the Discussion Paper and further recommend that the Privacy Act should explicitly recognise binding corporate rules as mechanisms for cross-border data transfers.** To avoid doubt, all these mechanisms should be included in the Privacy Act as optional and alternative mechanisms for APP entities to use; and such mechanisms should not preclude the use of other existing mechanisms under the Privacy Act. Having different and alternative mechanisms for APP entities to transfer personal information internationally affords them flexibility to configure their information processing procedures and resources in a manner that achieves greater cost efficiencies and relevance to their business models. This facilitates greater innovation and economic activity by organisations, both domestically and overseas, leading to more competitive consumer offerings while ensuring effective and appropriate protection for personal information.

9.5. We also remain open to a domestic third-party certification regime, provided it remains voluntary and does not preclude alternatives for demonstrating compliance (e.g., through the Cross-Border Privacy Rules (CBPR) or other international certifications).

9.6. The Discussion Paper proposes the removal of the express consent exception in APP 8.2(b). This exception allows entities to notify and seek express consent from individuals such that, if consent were granted, APP 8.1 would not apply to the disclosure of their personal information. In these circumstances the APP entity is not required to take reasonable steps to ensure that the overseas recipient does not breach the APPs.

We do not support the removal of the exception as it provides an alternative mechanism for data transfer in scenarios where alternative arrangements are not available, but the data transfer may be desirable, also from a consumer perspective.

For example, consider an Australian travel agency (the APP entity) providing travel booking services for Australians desiring to travel to a foreign country with a less

advanced privacy regime than Australia's. The travel agency would likely need to transfer personal information of travellers to entities in the foreign country (e.g., a hotel) to secure accommodation and/or transportation for the travellers. If the express consent exception were removed, and other transfer mechanisms/exceptions were not available for use by the APP entity in the circumstances, the travel agency might determine it too risky to assume liability and no longer provide the service. This would severely inconvenience and disadvantage travel consumers. It would be more useful, in our view, if required, to strengthen the information provision requirements to adequately inform individuals about the potential risks rather than potentially denying them the option of receiving a service.

Extraterritorial application

9.7. The Discussion Paper notes that the OP Bill includes an amendment to remove the requirements that personal information be collected or held in Australia.[9]

9.8. The proposed removal would have substantial implications, and we object to it on the following grounds:

9.9. Section 5B of the Act makes the following provisions for organisations and small business operators in relation to extraterritorial application

> *"(1A) This Act, a registered APP code and the registered CR code extend to an act done, or practice engaged in, outside Australia and the external Territories by an organisation, or small business operator, that has an Australian link.*
> *Note: The act or practice overseas will not breach an Australian Privacy Principle or a registered APP code if the act or practice is required by an applicable foreign law (see sections 6A and 6B)*
> *Australian link*
> *(2) […]*
> *(3) An organisation or small business operator also has an **Australian link** if all of the following apply:*
> *(a) the organisation or operator is not described in subsection (2);*
> *(b) the organisation or operator carries on business in Australia or an external Territory;*
> *(c) the personal information was collected or held by the organisation or operator in Australia or an external Territory, either before or at the time of the act or practice."* [emphasis added]

9.10. The draft OP Bill proposes to repeal paragraph 5B(3)(c).

The Explanatory Paper to the OP Bill notes as the reason for the proposed deletion:

> *"[…] when a breach of the Privacy Act occurs, it may be difficult to establish that these foreign organisations collect or hold personal information from a source in Australia. This is because large multinational companies may collect personal information from Australian customers from an entity that is not incorporated in Australia, and transfer it to other entities overseas for processing and storage. Similarly, foreign organisations may collect personal information about Australians but do not collect Australians' information directly from Australia, and instead collect the information from a digital platform that does not have servers in Australia and may therefore not be considered 'in Australia'.*

[9] p. 159, Attorney-General's Department, *Privacy Act Review Discussion Paper*, Oct. 2021

The Bill will remove the condition that an organisation has to collect or hold personal information from sources inside of Australia. This would mean that foreign organisations who carry on a business in Australia must meet the obligations under the Privacy Act, even if they do not collect or hold Australians' information directly from a source in Australia. For example, an organisation that collects personal information of Australians from a digital platform that does not have servers in Australia will more clearly be subject to the Privacy Act."[10]

9.11. However, the repeal of paragraph 5B(3)(c) would have far greater consequences as it reduces the 'Australian link' requirements – which trigger the extraterritorial application of the Act and registered codes – to effectively only one limb: to carry on business in Australia or an external Territory.

9.12. This would leave general Australian law as to interpretation of statutes which do not have express exterritorial provisions to determine the extent to which a non-Australian entity that carries on business in Australia is regulated in relation to acts and practices in handling of personal information of individuals that are outside Australia.

General Australian law does not provide clear guidance to enable the coverage of this amended provision to be reliably assessed.

9.13. The Act should continue to have the second limb, such that an organisation has to collect or hold personal information from sources inside of Australia. If the concern is that an organisation may indirectly collect or hold information that is derived from another source within Australia that directly collects or holds the information, section 5B could be amended to bring such indirect collection and holding within the definition. Otherwise, the change would create broad, uncertain and unconstrained extraterritoriality that is not consistent with good legislative practice and comity between national laws.

10. Direct right of action / statutory tort

Direct right of action

10.1. 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 Privacy Act is likely to lead to a large number of frivolous actions and predatory lawsuits which would further burden the Court system. 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.[11] This was despite the direct right of action being narrowly scoped in the CCPA.

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

10.3. If a direct right to action were to be implemented, it ought to be restrictively crafted. Among other things:

[10] p.22/23, Explanatory Paper, *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*, Nov 2021

[11] 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 limit for compensatory claims;**
- **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.**

Statutory tort

10.4. We observe from Chapter 26 of the Discussion Paper that the concern the AGD wishes to address through the possible introduction of a Statutory Tort is breaches of privacy instigated by individuals against other individuals,[12] 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 as such, we do not offer a view on which of the options presented in the Discussion Paper would best address this concern.

However, similar considerations to those outlined in paragraphs 10.1. to 10.3 above (introduction of a right of action) also apply to the creation of a statutory tort, namely, we are concerned that the creation of a statutory tort will lead to many frivolous actions and predatory lawsuits which may burden the court system and corporations targeted by such lawsuits. **We are opposed to the creation of a statutory tort for the invasion of privacy, as it would unintentionally capture entities already captured as APP entities under the Privacy Act.** We do not believe there is evidence that this tort is required.

11. Miscellaneous issues

Children and vulnerable individuals

11.1. In the communications industry represented by our members it is not uncommon for children to use devices and services on their parents' accounts. With the expanded definition of personal information, there may be cases where a communications service provider is unable to reasonably identify that a child is using its service through the parent's device. The proposals put forward in the Discussion Paper, to seek consent in situations where children are using a service, would have the unintended consequence, for example, that communications companies will have to gather more personal information (which they would not gather for other purposes) in order to verify the user's age, so as to determine whether or not parental or guardian consent is required.

11.2. We also highlight our significant concerns around the difficulties of age verification and parental/guardian consent verification put forward in our submission on the OP Bill.

[12] p.191, Discussion Paper, 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.

11.3. If one of the two options canvassed in the Discussion Paper must be progressed, we prefer Option 2 as it aligns with other international privacy regimes.

Employee records exemption

11.4. We recommend that this exemption be retained. We consider that workplace relations legislation, including the Fair Work Act and Work Health and Safety laws, effectively protect employee records, and that removing the exemption would create overlapping legislation, which in turn risks imposing conflicting (or at the very least confusing) obligations on employers.

11.5. The consultation goes into some depth to examine sensitive information separately from personal information. We consider the exemption on employee records should apply equally to personal information and sensitive information of employees (i.e., both types of employee information should remain exempt).

11.6. We do not agree with observations in the Discussion Paper that removal of the exemption is unlikely to increase the burden on employers.[13] While we agree that employers will have security measures in place to prevent inappropriate access, security does equate to privacy, and the burden created by removing the exemption is not related to security obligations; it is related to providing notification, seeking consent, responding to access requests and any new rights (e.g., opt-out rights) that are introduced in relation to personal and/or sensitive information.

Industry funding

11.7. We note that Chapter 24 of the Discussion Paper also questions how the OAIC may recoup the cost for expenditures required to adequately fund the operations of the OAIC. One of the options put forward in Proposal 24.7 includes "A statutory levy to fund the OAIC's investigation and prosecution of entities" (noting that the proposal limits this to entities that operate in an (undefined) high-risk environment).

11.8. Our members are open to discussing moderate fees to recover costs associated with educating and assisting APP entities to comply with the obligations of a revised Privacy Act on a fee-for-service model. **However, we strongly object to a statutory levy to fund the OAIC's investigation and prosecution of entities.**

It appears that application of the Act is so broad (economy-wide, a very large number of businesses) with such wide societal benefits that the operation of the respective regulator ought to be tax-payer funded and, hence, ought to be budgeted for by Government.

Overlap between APP5 and APP1

11.9. Proposal 8.4 looks to clarify when individual notifications are/are not required under APP5. This could be an opportunity to propose that an entity's overarching privacy policy statement could provide consumers with information about how/when information is collected, used and disclosed, thereby shifting away from relying on individual notifications under APP5.

11.10. We are also concerned that the amendment under proposal 8.4 does not allow for an exception where the effect of a notification may pose a serious threat to the life, health or safety of an individual or public health or safety. We suggest that an exception should be added along these lines.

[13] Discussion Paper, top of p.51.

Right to erasure of personal information

11.11. To the extent that a right to erasure is adopted, we recommend that it be made available only on a limited number of grounds, as is the case under Article 17 of the EU GDPR. Further, any right to erasure would require exceptions including:

- where the entity is required to retain the information by or under an Australian law or regulation, or court/tribunal order; and
- where deletion may be technically impractical or impossible.

Security and Destruction of Personal Information

11.12. We recommend not adopting proposal 19.3 of the Discussion Paper for the Privacy Act to be amended to require an APP entity to take 'all reasonable steps' to destroy or anonymise personal information when it is no longer needed or required to be retained by the APP entity. The change in standard from 'such reasonable steps as are reasonable in the circumstances' to 'all reasonable steps' will result in even greater ambiguity for businesses. It would be unclear whether the 'all reasonable steps' standard would be evaluated from what an APP entity can in fact do based on the existing circumstances and its systems, whether it would require an APP entity to implement new and costly technical capabilities to meet the standard. The change from 'de-identification' to 'anonymisation' will also result in an unworkably high standard to be met (as discussed above in paragraphs 4.29 through 4.37).

Implementation timeframe

11.13. We note that some of the changes contemplated in the Discussion Paper may have substantial implications for APP entities and urge the Department to ensure that any such changes are accompanied by a significant implementation timeframe for entities.

Such implementation timeframes ought to be enshrined (e.g. via commencement dates) in the legislation.

12. Conclusion

Communications Alliance looks forward to continued engagement with the Department 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 all stakeholders 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 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