COMMUNICATIONS
ALLIANCE LTD

Communications Alliance Submission

to the Attorney-General's Department on the

Privacy Act Review
Issues Paper

29 November 2020

Contents

1. Introduction

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

As consumers increase their use of online services to work, shop, communicate with family and friends or to be entertained, increasing amounts of personal information are being generated and captured by the providers of digital services. This information may become a target for malicious actors or misuse and as such, it is vitally important that this personal information – and hence the privacy of individuals – is protected to the greatest extent possible. As the Australian Competition and Consumer Commission's (ACCC) Final Report of the Digital Platform Inquiry (DPI) notes:

> *"The detriments suffered by consumers through decreased privacy and control over data can result in numerous additional harms ranging from receiving unsolicited targeted advertising to data breaches exposing their personal or financial information. These harms cause increased risks of online identity fraud and the potential for more effective targeting of scams. For instance, poor data security may expose consumers to greater risk of their personal information of being hacked or stolen, which may result in financial loss, reputational damage, and emotional distress."* [1]

Our members take privacy very seriously, and they support a privacy regime that protects the personal information of their customers and the 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. Therefore, we consider a review of the adequacy of the privacy regime as timely and necessary to ensure that all Australians can benefit from a robust privacy framework that reduces instances of malicious activity and misuse of personal information in today's digital age.

At the same time, in order not to hamper digital evolution, it is important that the privacy regime does not become unnecessarily burdensome for consumers and businesses alike.

Consequently, we believe it is important to foster an environment that allows businesses to innovate and provide services to the advantage of all Australians, or even a global audience, while at the same time safeguarding the privacy of individuals. We believe this balance can be struck, and the commentary contained in this submission seeks to reflect that balance.

About Communications Alliance

Communications Alliance is the primary telecommunications 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, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance. For more details about Communications Alliance, see http://www.commsalliance.com.au.

[1] ACCC, *Digital Platforms Inquiry Final Report.* p.444.

2. Discussion of Questions

Herein we offer feedback on some of the key areas for potential reform discussed in the Issues Paper.

While our members may have an interest in most or all of the questions raised in the Issues Paper, we have focused on some key issues as they pertain to the communications/ platform sectors.

Individual members of Communications Alliance may provide separate submissions to the Department.

2.1. Objectives of the Privacy Act

The objectives of the Privacy Act (Act) correctly emphasise that the protection of privacy ought to be balanced against the interests of entities when carrying out their functions and activities. This requirement for balance must not be dispensed of simply on the basis that achieving this equilibrium might be difficult in certain circumstances.

It is important to recognise that many of today's services or service attributes that consumers take for granted and would not want to go without are the result of innovation made possible by successfully balancing the legitimate interests of businesses – which could include fraud prevention, legal actions or security functionalities – with the right to privacy by individuals. It is, therefore, not appropriate to cast the right to privacy of individuals and business interests to use personal information as irreconcilable and incompatible positions that are, by default, at odds with each other.

Instead, as currently recognised by the second objective of the Act, these two 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 increased product and service offerings on the other. Removing the legitimate interest as one of the balancing factors when considering the use of personal information risks stymying innovation and investment in key areas of the economy.

If there are, indeed, tensions between the two interests and a perceived or actual difficulty in balancing those, then it would be more useful to consider means aimed at assisting to achieve a good balance between those interests rather than 'taking the easy way out' by simply abolishing the legitimate interest test altogether.

It is important to note that the European Union (EU) General Data Protection Regulation (GDPR) – which appears to influence much of the ACCC's thinking outlined in its Final Report of the DPI – deliberately includes a legitimate interest exemption for data controllers and third parties to balance the interests of individuals and businesses with the right for transparency and privacy of individuals.

A legitimate interest exemption also 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.

The DPI Final Report and the Issues Paper acknowledge the risk of 'consent fatigue' that could arise from the consequences of implementing a largely or purely consent-based privacy regime. The DPI Final Report only points to "considerable uncertainty and concern surrounding the relatively broad and flexible definition of the 'legitimate interests' basis for processing personal information under the GDPR" to argue for the exclusion of the legitimate interests exemption in an Australian context.

As set out above, we disagree with this reasoning: while the legitimate interests of organisations collecting and processing information may differ, the term does not offer a 'blank cheque' to process any information without consent.

In fact, one could argue that the Act ought to provide for a more flexible basis of processing recognising a business's legitimate interests for data processing that presents a reasonable risk to users, or is compatible with user's expectations, to process data beyond consent. Doing so would allow consent to be more narrowly focused on key issues and could contribute to a reduction in 'consent fatigue', as we will discuss further below.

2.2. Definition of personal information

As the Issues Paper highlights by tracing the history of the current definition of 'personal information', the definition is intentionally wide – but not all-encompassing, through the inclusion of the limitation that the information be "about an identified individual, or an individual who is reasonably identifiable".

The Explanatory Memorandum to the 2012 amendment of the Act and the definition of personal information stated that whether an individual is reasonably identifiable must be "based on factors which are relevant to the context and circumstances,"[2]. It also stated that the amendment was necessary to ensure the definition remained "sufficiently flexible and technology-neutral to encompass changes in the way that information that identifies an individual is collected and handled." As the Issues Paper correctly indicates, this "focus on 'identifiability' rather than 'identity' allows it to capture a broader range of information, including some online identifiers".[3]

We concur with the reasoning put forward in the 2012 Explanatory Memorandum and believe the current definition does not require amendment in order to continue to adequately protect personal information of individuals.

Following the case of *Privacy Commissioner v Telstra Corporation Ltd* (Grubb Case), the Office of the Australian Information Commissioner (OAIC) has released guidance[4] on the meaning of personal information with reference to 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.

Alternatively, to the extent the definition has not been able to accommodate the classification of certain technical and online identifiers as personal information, we believe it would be useful to consider the specific obstacles to such an inclusion and to remove those rather than creating a blanket inclusion of all online identifiers in the definition of personal information in the Act. This is because the classification of some technical identifiers is contingent on their linkage to an individual; in other words, it is not clear whether these identifiers constitute personal information in and of themselves.

For example, mobile operators collect, use and share customers' location information for the purpose of sending emergency alerts (e.g. in bushfire emergencies). This information as such should not be considered personal information (with potential attendant notification and consent requirements) unless it is linked (e.g. via account details) to a specific individual.

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. 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

[2] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, p. 53
[3] Attorney-General's Department, *Privacy Act Review Issues Paper*, 2020, p. 16
[4] As accessed on 26 Nov 2020: https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/

In its DPI Final Report, the ACCC recommended that "[t]he definition of personal information in the Act be updated to clarify that it captures technical data such as IP addresses, device identifiers, location data, and any other technical and online identifiers that may be used to identify an individual."[5] This recommendation seems to suggest that the information constitutes personal information as it may be used to identify an individual, instead of it only being personal information if it is actually used to identify an individual, or at the very least only when it is also held with additional information that makes an individual reasonably identifiable.

Overall, we believe that in the case of technical and online identifiers, neither the DPI Final Report, nor the Issues Paper, has sufficiently articulated the intended effect of an extension of the definition from 'information about an individual' to 'information that relates to an individual'.[6] For example, would a communication by a third party that describes another individual be enough to justify disclosure to that individual? How would the operator of a communications platform identify such a communication in seeking to respond to a request for such data?

It is important to understand and clearly articulate the desired outcomes of an extended definition of personal information: while such an extension may contribute to a more consumer-oriented approach to a definition of personal data, an extension will also make it more difficult for organisations collecting and using such data to navigate a more 'generic' – and potentially less clearly delineated – definition of such information. We would welcome further discussion on this matter.

Telecommunications data, is currently subject to strict use and disclosure rules under the *Telecommunications Act 1997* and the *Telecommunications (Interception and Access) Act 1979*. It is useful to highlight that the Australian Law Reform Commission (ALRC) has noted that Part 13 of the *Telecommunications Act 1997* potentially protects a broader range of information than personal information, including but not limited to the fact that the information protected under Part 13 can relate to individuals as well as organisations.[7] We also note that the information held by telecommunications providers not only relates to the individual who may request the disclosure of the information (and assuming informed consent) but may also include information relating to another individual (for example a telephone number that was called by the requesting individual) who has not necessarily given consent to the access of such information that relates to him/her.

In this context, we note that in 2017, Government conducted a review to consider whether data retained solely for the purposes of the data retention scheme (metadata) should be available for use in the civil justice system, and if so, in what circumstances. The review concluded that civil litigants ought not be allowed to access the data. In reaching this conclusion, Government considered evidence, amongst other issues, on the privacy of communications of unaffected individuals and the regulatory burden on the telecommunications industry in providing this data. It has not been articulated why a revised privacy regime ought to override those privacy considerations or, alternatively, how it would deal with these concerns.

If an amendment to the current definition of personal information is being pursued (noting our commentary around the need for a more detailed discussion above), the GDPR definition of personal data, i.e. "personal data means any information relating to an identified or identifiable natural person", could potentially provide a useful way forward. However, it is key that any future definition places circumstantial and contextual analysis at its core given the almost infinite variety of technical data and online identifiers and their uses, and is not incompatible with the GDPR definition. Any form of listing of types of online identifiers considered to fall within the definition ought to be avoided as it risks diluting the

[5] ACCC, *Digital Platforms Inquiry Final Report, June 2019*, p. 459.
[6] The case *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC established that the latter definition of 'information that relates to an individual' was wider than a definition that used 'information about an individual'.
[7] Refer to https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/71-telecommunications-act/interaction-between-the-privacy-act-and-the-telecommunications-act/

circumstantial and contextual approach. Such listings are also unlikely to withstand the rapid dynamic evolution of technical data and online identifiers and risk becoming outdated relatively quickly.

2.3. De-identified, anonymous and pseudonymous information

Definitions of personal information typically include identified data or data that relates to a specific individual (e.g. name, email, etc.). Many laws, including the GDPR, also cover pseudonymous data, such as information tied to a device or cookie ID. Many global entities have generally adapted to these broader definitions, provided the substantive obligations that apply to this information are reasonable.

If a revised Act was to afford additional protection to de-identified, anonymous and pseudonymous information, the substantive obligation (e.g. access and portability) ought to make a distinction between these types of data and identified data in order to reflect that these rights cannot be safely applied to pseudonymous data. Any definition of personal information ought to avoid an inclusion of 'household data' and public data, or other sources of data that are not about a specific individual or device.

Generally speaking, and in line with our remarks on the necessity of a legitimate interest basis for processing information, the Act ought not unnecessarily add regulatory and operational burden to businesses processing information where information that has been de-identified, anonymised and/or pseudonymised no longer poses a risk to the privacy of an individual.

2.4. Inferred personal information

The Issues Paper also seeks views on whether a revised Act should offer protection for inferred information. The Paper correctly highlights that "APP entities may find it difficult to practically determine the point at which the inferences they generate become personal information".[8]

The GDPR does not conclusively state that inferred data is or is not personal data. Further case law is required to establish important distinctions for inferences (and the reasoning and processes that lead to inferences) in relation to a potential classification as personal data. However, Article 20 of the European Union (EU) *General Data Protection Regulation*, as interpreted in the *Guidelines on the right to data portability* (16/EN WP 242 rev.01 dated 5 April 2017) as adopted by the former Article 29 Data Protection Working Party, specifically excludes inferred data or derived data as created by a service provider, but potentially includes cleansed data and customer-specific aggregations and representations of transactional, customer-volunteered or customer-provided, and provider-observed data.

Consequently, we believe that the definition of personal data should also not explicitly include information that is imputed, derived or inferred. Further, data that is not able to be re-identified to an individual in the normal course of business within a data holder should not be considered personal information.

2.5. Notice of collection of personal information and consent to collection, use and disclosure of personal information

Generally speaking, the consent requirements of the Act ought to be based on what is reasonable in the circumstances and rest on the principle of obtaining express user agreement with notice in a limited set of cases. A narrow approach to notification, i.e. a limited number of scenarios that trigger notification, and a broad basis for consent are preferable over a prescriptive approach (possibly even involving '1 tick-box per statement/purpose') as the former is more likely to

[8] Attorney-General's Department, *Privacy Act Review Issues Paper*, 2020, p. 16

- Avoid 'consent fatigue';
- Promote innovation; and
- Allow regulators and enforcement bodies to focus on key issues.

Consequently – and following on from our discussion of legitimate interests above – we are concerned about a regime that relies on overly burdensome consent (for consumers and for businesses) as the basis for consumer permission to collect, process or use personal information.

An approach to consent that "[r]equire[s] consent to be obtained whenever a consumer's personal information is collected, used or disclosed by an APP entity, unless the personal information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason"[9], as previously advanced by the ACCC, is, in our view, impractical and also undesirable from a consumer, business and economy-wide perspective.

Independent of our concerns highlighted above, any privacy regime ought to be very clear that notification and consent, where required by the regime, could be complied with through an express notice/informed consent at the beginning of a customer relationship/contract and do not require individual notifications/informed consents each time personal data is being collected.

We note that the limitation that consent is not required where the information is necessary for the performance of a contract may not be helpful in all circumstances as it may be difficult to differentiate whether information was necessary for the performance of a contract or only helpful for this purpose, or what exactly constitutes 'the performance of a contract'.

We propose that, in addition to other means of seeking consent, one further consumer-convenient mechanism for businesses to fulfil their notice and consent requirements (where consent requirements indeed apply) could be through adjustable privacy settings in personalised account portals or similar (e.g. 'My Account') where individuals can freely access and customise their preferences at any time during their contractual relationship with the business.

In any case, it will be imperative that the definition and interpretation of notice and consent are not inconsistent with (and do not go beyond) the respective definitions of the Australian Consumer Data Right (CDR) and GDPR.

In this context it is key to highlight that Article 6 of the GDPR recognises six bases for processing personal data, with 'unambiguous consent' only being one of those bases. Most notably, as indicated above, the GDPR recognises the legitimate interests of businesses to process data as well as the necessity to process such data for the preparation and execution of a contract. (The other three bases include data processing where it is required to comply with a legal obligation, to save a person's life, and a public interest test.)

It is also important to realise that the application of the legitimate interest test ought to be a genuine option for businesses and must not be unduly constrained by guidance along the lines of 'play it safe – seek consent' if the privacy regime seeks to avoid notification and consent fatigue. The flood of 'cookie notices' that every user of the internet experiences since the introduction of the GDPR may serve as an example of the (by most users undesired) consequences of consent requirements and/or the desire by businesses to avoid potential scrutiny or enforcement action where legitimate business interests are being discouraged as a basis for data processing.

Consequently, given the amount of data that is being 'produced' and processed in fully digital societies, only a privacy regime based on a pragmatic approach which focuses individuals' attention on key risks to their privacy (rather than a dogmatic approach with

[9] p.456, ACCC, *Digital Platforms Inquiry Final Report*, June 2019

consent for each specific processing activity at all times) will be successful in keeping consumers engaged and safeguarding individual privacy.

2.6. Obtaining consent from children

Children are amongst the most vulnerable consumers in our society while at the same time being very engaged with digital media. Consequently, it is important to ensure that children understand when their personal information is being collected and for what purpose.

Children are less likely to engage with solely text-based approaches that aim at safeguarding their privacy, especially where these may involve more complex language. Therefore, we believe an approach involving plain English and infographic-styled descriptions of the privacy implications that an organisation's data collection activities may have for their privacy could be explored.

We would also welcome clarity around the definition of 'minor' for the purposes of this discussion.

2.7. Third party collections

In its DPI Final Report, Recommendation 16(b), the ACCC proposed to "[r]equire all collection of personal information to be accompanied by a notice from the APP entity collecting the personal information (whether directly from the consumer or indirectly as a third party), unless the consumer already has this information or there is an overriding legal or public interest reason."[10] This recommendation appears to suggest that such notification is to be provided at the time of collection.

Irrespective of the absence of a legitimate interest exemption in this recommendation, we also note that the current Act recognises that an immediate notification requirement is not practical in many circumstances – for example where the collecting entity is a third party and does not own or operate the website it collects the data from – and, consequently, allows for notifications after collection where it is impractical to do so at the time of collection.

Where multiple entities are collecting information, the proposed recommendation may create a situation of 'notification overload' for consumers who might be receiving numerous notifications at the same time. This bears the risk of disengagement – the opposite outcome of what a well-designed privacy regime intends to achieve.

Some members, therefore, consider that one approach could be, in certain circumstances to require the third-party operator of a website to provide the required information, either via a notice or another suitable means, instead of the APP entity performing the primary service that the customer contracted for. The following example may illustrate such a circumstance and proposed approach:

> A consumer has a direct relationship with WidgetCo. WidgetCo is the APP entity that has fulfilled its obligations with respect to the Privacy Act for any direct personal information it obtained as a part of the consumer becoming a customer.
>
> However, WidgetCo does not provide first-hand technical support for its products or services. Instead, WidgetCo may engage a third party, HelperCo, to provide that assistance.
>
> HelperCo, in turn, uses a platform-as-a-service (PaaS) solution in order to create 'support tickets'. The ticketing process may, out of necessity, require the collection of personal information in order for the assistance to be provided.

[10] ACCC, *Digital Platforms Inquiry Final Report*, June 2019, p.456

When the customer requires support for a WidgetCo product or service, he/she may visit the WidgetCo website, select a 'Support' option, and subsequently be re-directed to the PaaS where HelperCo will manage the tickets.

Whilst WidgetCo would qualify as an APP entity (with the customer relationship), HelperCo and the PaaS provider may or may not be an APP entity. Either way, in many instances, WidgetCo may have no awareness, nor even necessity of awareness, of the customer obtaining technical support (or the customer's personal information). Yet, the personal information is being collected by the PaaS for access by HelperCo.

Under the above (commonplace) scenario, in our view, HelperCo should work with the PaaS provider to ensure appropriate notice is provided regarding the collection of personal information, and the purposes for which it is being collected. This could be accomplished with a simple disclosure during the ticket creation process.

Doing so would inform the customer that a third party is collecting the information and the reasons for doing so, without a direct necessity for WidgetCo to have full visibility of the process and to provide notification itself.

In an alternative approach contemplated by some members – and building on the above example – a single notice at the beginning of the contractual relationship could be provided by WidgetCo without the need for further notices by HelperCo and/or the PaaS provider.

Considerations for instances where businesses are unable to notify a data subject of the collection of their data (Question 23 of the Issues Paper) ought to be guided by similar practical deliberations: given the broad concept of 'collection', there are many situations where a business may need to share personal information with a third party contractor (e.g. for data storage, to help with customer administration, data analysis, reporting etc.). To require those third parties to notify the data subject would likely cause confusion to the data subject (who may not understand the reason for the notification) without a clear benefit to the data subject. Entities would normally cover 'sharing' of data and the limited purpose of such 'sharing' in their privacy policies.

2.8. Processor/Controller distinction

The Act currently does not contain – and the Issues Paper does not discuss – a distinction between data controllers and data processors (as, for example, present in the GDPR).

As highlighted by the matters discussed in the previous sections, we believe that the revised Act would be improved by incorporating such a distinction to clearly allocate responsibilities pertaining to notification, consent and security (including destruction and de-identification) of personal information to the entity that is best placed to handle those. This would also assist with minimising duplication of effort for businesses (complying with obligations) and individuals (dealing with duplicative notices and requests for consent) and would serve to enhance transparency for participants of the regime.

2.9. Standard notices or icons

The reasons for collection of personal information, the subsequent use cases for such data and the variety of businesses engaging in the collection and processing of personal information are manifold. Therefore, it may be, at times, challenging for consumers to quickly understand why their personal information may be collected and what the information is being used for.

We would welcome engagement with all stakeholders on finding meaningful ways for consumers to easily discern key uses and reasons for data collection, including through the use of icons.

From a practical perspective we note that the large number and variety of organisations collecting personal information and the various use cases of such information may make it challenging to develop a standardised approach. Consequently, we would welcome additional detail, potentially for inclusion into the Discussion Paper that is foreshadowed to follow this Issues Paper in 2021.

2.10. Right to erasure, destruction and de-identification of information

APP 11.3 provides for the destruction or de-identification of data once the data is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs (unless retention of the data is required by law) and, consequently, already goes some way to ensuring that personal information is not kept unnecessarily.

While a right to erasure (or even a 'right to be forgotten') may be appealing in certain circumstances, we urge all stakeholders to carefully consider any unintended consequences that such a right may have.

As previously indicated, telecommunications providers are subject to a variety of different obligations in relation to the privacy of their customers, including the non-disclosure obligations of the *Telecommunications Act 1997* and the *Telecommunications (Interception and Access) Act 1979*. These providers also face a myriad of obligations to retain/preserve data for a variety of purposes, e.g. accounting, reporting, complaint handling, law enforcement, provision of emergency call services etc.

For example, our industry is required to collect and retain data under legislation, such as the Data Retention legislation, where these obligations are not tied to an entity's status as an APP entity. It needs to be clear that data retained under such legislation would be exempt from a proposed erasure requirement, independent of an entity's APP status and of whether the data retained is personal data or de-identified.

We suspect that other sectors are similarly subject to a range of privacy and data retention/preservation regulations. Consequently, any discussion of a right to erasure requires a careful economy-wide analysis of requirements, operational needs and technical feasibility, not only for APP entities but potentially also entities that may not be subject to the Privacy Act but rely on some or all of the data that would be subject to the right to erasure. A discussion of this right also ought to include a thorough cost-benefit analysis.

Noting that a right to erasure, as we understand it, would not dispense with the requirements of APP 11.3 to destroy or de-identify the personal information once it is no longer needed for the disclosed collection purpose (or under law), we believe that consideration would also need to be given to the question of whether the right to such erasure could be waived by data subjects and whether such waivers would be revokable. In a similar vein, we are mindful that consumers may request the erasure of their data but may later regret their decision as the continued existence of their information would have had future benefits that they did not anticipate or, alternatively, that the erasure of their information does not allow them to proceed with an online transaction or complaint that would have required an entity's access to their erased data.

2.11. Duplication and inconsistency of legislative instruments

As the discussion of the definition of personal data and a right to erasure highlight, our industry is subject to multiple legislative instruments in relation to privacy. The multiplicity of obligations leads to duplication and, at times, potential inconsistency and uncertainty with respect to requirements.

We, therefore, agree with the Department of Communications (now Department of Infrastructure, Transport, Regional Development and Communications) recommendation, aimed at reducing duplication and unnecessary regulatory burden:

"Repeal most of Part 13 of the Telecommunications Act. Provisions in the Privacy Act would continue to regulate the use and disclosure of personal information handled by telecommunications providers.[…] Prohibitions on the disclosure of telecommunications information to law enforcement agencies would be retained, except where otherwise authorised by law or under a warrant. Consequential amendments to the Telecommunications (Consumer Protection and Service Standards) Act 1999 may be necessary to ensure that it is clear that disclosure of information can continue to support disclosures in the public interest (for example, to protect a person's life)."[11]

2.12. Access to information

In general, individuals ought to have access to their personal information. However, it is also important to note that not all personal information can be easily accessed by the collecting entity, potentially as the collection of such data may be a by-product – but necessary action – in the performance of a contract.

Accordingly, Article 29(2) of the New Zealand *Privacy Act 1993* provides for an exemption to access where personal information is not 'readily retrievable'. 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."[12]

A similar limitation on access ought to be included into the Australian Act.

2.13. Overseas data flows and interaction with other regulatory regimes

The global nature of open economies, combined with data flows as the indispensable basis of almost any economic activity, make it imperative to strive for and achieve the greatest possible extent of interoperability of privacy regimes.

As indicated in the Issues Paper, the notion of adequacy, i.e. mutual recognition that the protections of a foreign privacy regime are adequate, is a key enabler for such interoperability where one common regime that covers all economies across which data is being processed and/or transferred cannot be achieved.

Consequently, we are generally open to discussions around efforts that would move the Australian regime closer towards adequacy with respect to the 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

[11] Department of Communications, *Consultation paper: Proposed measures for the Telecommunications Deregulation Bill No. 1,* 2014 April 2014
[12] As accessed at 26 Nov 2020: https://privacy.org.nz/further-resources/knowledge-base/view/261?t=101292_142086

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.

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. One way of enhancing clarity in this regard would be for the Act to expressly clarify that data and server localisation are not required for entities to meet their 'accountability' obligations in transferring personal information overseas.

With respect to the exception to extraterritorial application of the Act in relation to acts or practices required by an applicable foreign law, we believe that no change to the current Act is required. That is, the exception ought to be retained to minimise instances where entities may be faced with the choice of breaching one jurisdiction's obligations in order to comply with another one's.

Against the background of the recent 'Schrems II' (preliminary) ruling of the Court of Justice of the European (CJEU), we also point to potentially existing frictions of the GDPR and Australian law more generally, including existing and pending Australian legislation that may be considered not containing sufficient limitations to ensure proportionate use of personal data by security agencies and not granting data subjects appropriate actionable rights before the Courts.

Where tensions between different Australian legislative regimes arise, we would welcome a holistic approach to the design of those regimes which not only recognises the potential tensions between the objectives of those different regimes but also offers a practical solution to dealing with these competing objectives.

2.14. Third party certification

Members are yet to fully consider the question of a domestic privacy certification regime. At this stage we tentatively offer our opinion that a domestic privacy certification scheme could be welcome as it provides APP entities with a mechanism for demonstrating their compliance with the Act. However, such a scheme needs to remain voluntary as there may be other ways of demonstrating compliance (e.g. through the Cross-Border Privacy Rules (CBPR) or other international certifications).

2.15. Enforcement powers under the Privacy Act and role of the OAIC

Overall, we believe that the current enforcement powers and the role of the OAIC are appropriate. The remedies and enforcement mechanisms available to the OAIC are, in our view, sufficient and do not require expansion.

However, we do note that it appears, at times, the OAIC would benefit from additional resources to allow deeper engagement with industry participants on a regular basis. This would allow the OAIC to gain an early understanding of issues as they arise from a multi-stakeholder perspective.

2.16. Direct right of action and statutory tort

A direct right to action (as well as the introduction of a statutory tort) has been subject of various previous debates. While we have not been presented with compelling evidence that such a right is indeed needed, our members are open to further discussion and are keen to

understand which issues – and whether those can be distinguished on a sectoral basis – the introduction of such a right seeks to remedy.

Our members are concerned that introducing such a right is likely to lead to a large number of frivolous actions and predatory lawsuits. Without prejudice to the outcome of any future engagement on this matter, we believe that any disputes over a breach of privacy obligations first ought to proceed through the OAIC for conciliation prior to opening any potential avenues for direct action. If additional resourcing at the OAIC is required to effectively discharge of this role, then resourcing arrangements ought to be reconsidered. In addition, we believe that a direct right to action, if implemented, ought to be accompanied by a reasonable limit for compensatory claims. Consumers also can complain to the Telecommunications Industry Ombudsman for certain types of privacy breaches.

It should also be noted that pursuing claims through Courts is an inherently slow and costly mechanism for dealing with privacy issues, especially where the Court system is 'clogged up' with cases that ought not have been pursued through the Courts in the first place.

Similar considerations as those outlined in relation to a direct right of action apply with respect to the proposed introduction of a tort. A statutory tort was proposed by the Australian Law Reform Commission (ALRC) in 2014 but did not progress largely on the basis that it was recognised that the existing privacy and other laws in Australia provide significant consumer protections for serious invasions of privacy. We have seen no evidence of a convincing explanation as to why the arguments that led to that conclusion are no longer valid or would be overridden by other arguments today.

Further judgement of the proposal to introduce a tort is also hampered by the lack of a definition of 'serious invasion of privacy'. Additional detail around and relative weight of the public interest considerations that are being mentioned as a balancing factor in the tort debate would also be helpful.

Consequently, we welcome additional detail on the issues that the introduction of a direct right to action and/or a statutory tort seek to address, as well as specific guidance on how such a right/tort would operate in practice.

2.17. Notifiable Data Breach scheme

Our members do not advocate for any major changes to the existing Data Breach Notification (NDB) scheme.

Some members have indicated that the OAIC guidance on when an incident ought to be classified as a NDB would benefit from further clarification, including in relation to personal data held on a consumer device which comes into the possession of a telecommunications provider.

We would welcome engagement with the OAIC on these matters.

3. Conclusion

Communications Alliance looks forward to continued engagement with the Attorney-General's Department, the Office of the Australian Information Commissioner and other stakeholders on the review of the Privacy Act to ensure that any future privacy regime is fit-for-purpose, sufficiently flexible to adapt to the rapidly changing digital environment, globally interoperable and practical for businesses and individuals alike.

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