TELSTRA CORPORATION LIMITED

TELSTRA HEALTH PTY LTD

Attorney General's Department Issues Paper

Review of the Privacy Act

27 November 2020

Executive Summary

At Telstra and Telstra Health, we are committed to protecting the privacy of our customers, suppliers and employees, and to keeping their personal information safe, because we know how important it is that people trust us. Because of this, we welcome the opportunity to respond to the Attorney General Department's issue paper *Review of the Privacy Act*.

The current principles-based regime should be maintained

Few people in 1988 could have foreseen how the incredible advances in technology over the past three decades would transform our lives into today's online world of communicating, conducting business, working from our homes rather than offices, online shopping and social media. And yet, the principles enshrined in the Privacy Act 1988 (Cth) to protect consumer's privacy, ensure they are informed, and can provide or withhold consent for the collection or use of their personal information, are as relevant today as they were then. Principles serve as a foundation for a system of behaviours that can accommodate rapidly changing markets and technologies, providing a relevant framework for businesses and consumers to use. Unlike highly prescriptive regulation, principles-based regulation avoids becoming outdated or irrelevant as the environment changes.

The vast majority of the Privacy Act is appropriate and of a necessary standard

We consider much of the Privacy Act to be fit for purpose although there is scope for developing or updating guidance in some areas. We see no need for changes to aspects of the legislation such as the definition of personal information, protections for de-identified, anonymised or pseudonymised information, notification, consent, control or security, or consumer redress such as the introduction of a statutory tort or direct right of action. However, in many of these cases, we agree there is scope for additional transparency and/or guidance which can be achieved through updates to accompanying Regulator guidelines. The benefit of providing additional clarity through Regulator guidelines is that it can be continuously updated to evolve with changing technology. We remain in strong support of a principles-based, technology neutral regime.

If changes are to be made, there must be consultation

One question posed by the AGD is whether Australia would be served by seeking adequacy under the GDPR. While in general we support regulation designed to facilitate global, secure free-flow of data and increases in global regulatory consistency, we have concerns that this is a nuanced topic with many potential flow-on effects and considerations. If the Government is serious about pursuing GDPR adequacy, we request further consultation and additional information on what the Government considers adequacy would entail.

Finally, we observe there is a raft of different Commonwealth legislation which govern different types of personal information on top of the Privacy Act. We strongly recommend a holistic review be undertaken on all these laws to ensure consistency and remove overlapping laws, where possible.

Table of Contents

01 Introduction

Consumer sentiment is changing. The ACCC, in quoting the Productivity Commission's Data Availability and Use Final Report[1] observes that:

> *Social licence will develop if people:*
>
> - *have a sound basis for believing in the integrity and accountability of entities (public and private) handling data*
> - *feel they have some control over how their own data is used and by whom, and an inalienable ability to choose to experience some of the benefits of these uses themselves*
> - *better understand the potential community-wide benefits of data use.*

We are committed to protecting the privacy of our customers, suppliers and employees, and to keeping their personal information safe. Because of the importance we place on privacy and protecting our customers' data, we welcome the opportunity to respond to the Attorney General Department's (**AGD**) issue paper *Review of the Privacy Act* to help frame the conversation.

Our submission is structured as follows:

- Section **Error! Reference source not found.** sets out our views that the Privacy Act must remain a principles-based regime;
- Section **Error! Reference source not found.** identifies areas of the Privacy Act where we believe legislative changes are not required, although in some cases, we note additional guidance will help or we agree with the need for better transparency;
- Section 04 identifies areas of the Privacy Act where we recommend further consultation should there be a desire to amend the Act; and
- Appendix 1 contains answers to selected questions from the issues paper where we consider further detail (beyond that in the body of our submission) is warranted.

02 A principles-based regime is sufficient and appropriate

In many respects, the GDPR has moved with social sentiment toward greater protection for the privacy of individuals, and we recognise this change in community attitudes. At the same time, the GDPR seeks to balance consumer rights with the need for businesses to operate efficiently and effectively by acknowledging that there are legitimate business interests for processing personal information. For instance, the GDPR recognises that processing of personal data is lawful when it is necessary for the legitimate interests of the controller or third party. Some examples given include fraud prevention, ensuring IT security and direct marketing.

To achieve this balance, we strongly believe the Privacy Act must be framed through a set of principles. The AGD observes the Privacy Act was drafted to be principles-based, technologically neutral and supported by detailed regulatory guidance. The AGD notes[2] this is best demonstrated in the second reading speech of the then Attorney General, the Hon Lionel Bowen MP who spoke of the "*enormous developments in technology for the processing of information*". We agree with the AGD's observation,

1 ACCC Digital Platforms Inquiry Final Report, p.22.

2 Issues Paper, p.13.

and consider that other parts of the Hon Lionel Bowen MP's speech go clearly to a principles-based regime:

> *The scheme of the privacy Bill is to enunciate a series of rules, called information privacy principles, which are based on the principles recommended by the Law Reform Commission in its draft legislation. … An agency collecting personal information from the individual to whom the information relates must see that that person is generally aware of such things as the purpose for which the information is being collected, … The principles require agencies, when both collecting and retaining information, to see that it is relevant to the purpose of collection, up-to-date and complete. … The principles require agencies to store information records securely against loss or misuse.* [3]

In over thirty years since, these principles are still accurate and relevant, and we remain in strong support of a principles-based, technology neutral regime. Technology will continue to advance in ways that we cannot predict today, and believe the Privacy Act was ahead of its time in enshrining what continues to be a successful, principles-based approach that will best serve consumers and businesses by creating a fair and equitable regime that is implementable, manageable and robust.

2.1. A principles-based regime recognising business interests as well as privacy interests of individuals will best serve the needs of consumers

The protection of individuals' privacy is not incompatible with the interests of businesses. Allowing businesses to operate efficiently and effectively can lead to real benefit for the consumer by way of innovation and offerings better tailored to meet their needs. It is always in the interests of businesses to appropriately protect the privacy of their customers to both retain and grow their customer base. However, if the needle is moved too far in the direction proposed by the ACCC in its Digital Platforms Inquiry Final Report (DPI Report), it could result in increased regulatory burden on businesses impacting their ability to operate flexibly and innovate, with minimal (if any) meaningful benefit to consumers.

The key reason provided for considering the removal of the Act's second object is around the growing use of data analytics by businesses. We believe the current privacy framework provides adequate protection in this regard through the Australian Privacy Principles (APP) requirements around transparency, notification, security and access. If there are concerns that some businesses may not be complying with their APP obligations because of the "tension" referred to in the Issues Paper, then this should be managed through use of the Regulator's enforcement powers, more guidance from the Regulator and/or the development of a Code of Practice for industries of concern.

Other comparable privacy laws recognise legitimate business interests which need to be considered together with an individual's right to privacy. For instance, the GDPR specifically provides for a legitimate interests exception by recognising that lawful processing can take place where necessary for the "*purpose of legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data*."[4]

---

3 Commonwealth, *Parliamentary Debates*, House of Representatives, 1 November 1988, 2117 (Lionel Bowen, Attorney-General).

4 Article 6 (1)(f).

Further, we hold the view that delivering higher consumer privacy protection is an opportunity for those businesses who embrace higher levels of protection. For example, Apple® recently announced[5] that from 8 December 2020, developers of applications (apps) will be required to provide information about the app's privacy practices, including the practices of third-party partners on the App Store® for consumers to view prior to downloading the app. This has the potential to attract privacy conscious consumers to the Apple® ecosystem if consumers perceive their privacy will be better protected.

In the New Zealand Privacy Act 2020, one of its purposes acknowledges that at times consideration may need to be given to rights and interests other than privacy interests of the individual and the NZ Commissioner is required to have regard to other interests including "*government and businesses being able to achieve their objectives efficiently*"[6] in carrying out his statutory functions.

To this end, the objects of the Privacy Act are critically important for setting the intent of the Act. The objects of the Act acknowledge the need to strike an appropriate balance between the protection of the privacy of individuals with the business interests of entities. We support the existing objectives of the *Privacy Act 1988* (Cth) (**Privacy Act**), which strike this balance in a technology-neutral, principled way.

03 Most of the Privacy Act appropriate and of a necessary standard

The principles-based approach to the development of the Privacy Act discussed in the previous section has resulted in an Act that has stood the test of time, and we consider remains fit-for-purpose. In this section, we explore aspects of the Act that we judge to remain effective, albeit that in some instances updating supporting guidelines will assist businesses better understand how to implement the requirements of the Act.

3.1. The current definition of personal information is sufficient, including catering for inferred personal information

It is well established that the same piece of information may or may not be personal information depending on the context and specific circumstances.[7] If a piece of technical information reveals something about an individual who is reasonably identifiable then it will be personal information, so no change is needed to the definition. The OAIC has already provided guidance[8] on the meaning of personal information with reference to the Grubb case. We suggest if there is confusion on when technical information can be personal information versus other scenarios where it is not, this could be covered in additional OAIC guidance (which can be updated as technology evolves to cover new types of technical information).

The key risk is that a change to automatically capture technical information, such as Internet Protocol (IP) addresses, device identifiers and network metadata would have unintended consequences. For example, it may interfere with the ordinary interactions required between different network operators for their networks to interoperate. If this type of information is not being used by the network operators in a

5 App privacy details on the App Store. https://developer.apple.com/app-store/app-privacy-details/

6 s.21 of the NZ Privacy Act 2020

7 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) s.53 and *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 63

8 https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/

way that has an impact on any individual from a privacy perspective, then there may clearly be a cost to business without any corresponding gain for consumers – it would not strike the right balance.

The Issues Paper also considers whether information about an individual's activities (e.g. transaction history or 'likes' on a social platform) can be used to infer information about that individual, and if so, whether the definition of personal information should be updated to expressly include "inferred personal information". We consider that if new information of this type is created about an individual, it is already captured under the existing definition of personal information. In its guidelines on the meaning of "personal information" the OAIC even provides the following as a "common example" of personal information:

> *Information or opinion inferred about an individual from their activities, such as their tastes and preferences from online purchases they have made using a credit card, or from their web browsing history.*

If the definition of personal information is amended to expressly capture inferred personal information, we are concerned it may trigger unintended consequences such as additional notification and consent requirements

Regarding personal and sensitive information in the health sector, we encourage consistency of concepts and definitions as far as possible across the Commonwealth Privacy Act, State and Territory privacy legislation, the Healthcare Identifiers Act and My Health Records Act. For example, definitions relating to health data and its use for genetic analysis are unclear and inconsistent. Definitions and permitted uses of data relating to organ donors on the Privacy Act, Health Identifiers Act and Medical Health Records Act are also inconsistent.

Simplicity and consistency of these rules has wide ranging benefits - for clinicians at the point of care, researchers, and for industry as suppliers of systems that design manage controls for these data across jurisdictions.

3.2. No need for additional legislated protections for de-identified, anonymised or pseudonymised information

Information that has been de-identified should no longer be regarded as personal information and, therefore, should not be regulated under the Privacy Act as its use or disclosure should have no privacy-related consequences for any individual.

Any reforms intended to clarify this position should stop short of imposing a higher standard of "anonymisation" whereby de-identified data may continue to be personal information until all possibility of re-identification has been eliminated. Given the practical challenges of achieving that standard, any such change could have a chilling effect on innovation whereby useful research and analytics currently carried out with very low risk to privacy could be prevented simply because it is not possible to absolutely eliminate all possibility of re-identification.

We observe the OAIC has already provided guidance on what constitutes de-identified or anonymised information[9] and we consider an appropriate solution, should further clarification or guidance be required would be to update this guidance. Updating supporting information such as accompanying guidance is an appropriate mechanism, as it can be updated again in the future as technology evolves further.

3.3. No need for legislative changes to notification

We support the ACCC's recommendations about improving transparency and limiting the information burden on consumers through "best practice" notices including, where applicable, multi-layered notifications and the use of standardised icons or illustrations. We believe competitive industries will, by necessity, move to this approach, as an innovative way of engaging with customers.

However, we do not support the recommendation that the notification requirements in the Privacy Act be amended to require all collections of personal information to be accompanied by a notice from the APP entity collecting the personal information (whether directly from the consumer or indirectly from a third party), unless the consumer already has this information or there is an overriding legal or public interest reason.

The current APP 5 notification requirement is for an APP entity to *"take such steps (if any) as are reasonable in the circumstances"* either to notify the individual of certain matters or otherwise ensure they are aware of those matters. As noted in the Issues Paper, the Explanatory Memorandum to the introduction of the APPs in the Act explains that this language was used to provide flexibility given the broad range of APP entities and functions/activities regulated under the APPs.[10] We believe retaining this flexibility is important for the reasons below.

It is not uncommon for organisations to engage specialist contractors to assist them with their business operations, for example, printing houses to print customer bills or IT helpdesks to help resolve customer IT complaints. It is hard to see any benefit to consumers of requiring collection notices each time personal information was shared in these types of circumstances. The purpose for which the personal information is being used has not materially changed and the risk of a consumer getting "notification" fatigue from receiving multiple notices is high (and seems to contradict the ACCC's finding that the vast majority of consumers do not read the privacy policies and other terms and conditions presented to them by digital platforms).[11]. It could also lead to an increased sharing of consumer contact personal information so these entities can send notices (even if they didn't need that information to provide the specialist services).

The ACCC's recommendation would also mean notification is required to be given to an individual even when that individual's personal information was provided by a third party and the APP entity has no relationship with the individual. There are legitimate circumstances when an APP entity may receive personal information of an individual indirectly. In those circumstances, the APP entity relies on the third party to notify the relevant individual. The most common is that of authorised representatives on an account. The APP entity would normally only need a small amount of personal information for that

---

9 OAIC Guide on De-identification and the Privacy Act, available at: https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act This guide is helpfully complemented by the De-identification Decision-Making Framework, jointly developed with CSIRO's Data61, available at https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-decision-making-framework/

10 Privacy Amendment (Enhancing Privacy Protection) Bill (Cth) 2012.

11 ACCC, *Digital Platforms Inquiry Final Report*, p.396

purpose. If the ACCC's recommendation was implemented, the APP entity would need to obtain full contact details of that representative to send them a notice.

In our view, given a notification obligation already exists, it would be preferable to ensure that operators who currently take a limited, non-customer centric approach are encouraged to meet the transparency requirements in the existing legislation, rather than overhauling the privacy regime in this regard.

The focus of any reforms on notification should focus on ensuring that notices are only provided where they are meaningful (i.e. where there is a change that may legitimately prompt a consumer to change their behaviour), rather than requiring notices where they would not serve a useful purpose and may, in fact, be detrimental from a consumer perspective. We would support more Regulator guidance on different ways to improve transparency.

3.4. Consent should be only one of the lawful bases for use

We consider that requiring consents be unbundled is consistent with the proposition that consent should be specific. However, without other valid legal bases for processing information besides consent, it is also likely to result in consumers being swamped with requests for consent. That will not necessarily drive meaningful engagement by consumers on privacy-related issues and, therefore, will not necessarily be good for consumers.

A better approach would be to retain consent as just one of a number of equally legitimate legal bases for processing personal information, perhaps with a special role to play in relation to higher sensitivity processing activities (e.g. in relation to collection and use of health or other sensitive information, as is currently the case). This is consistent with the GDPR, which provides for "legitimate interests" as a lawful basis for processing personal data, alongside consent and other lawful bases. In this case, requiring that consents be unbundled in order to be valid would make sense, would provide choice and control to the consumer (i.e. a customer-centric approach) and would reflect the special role that consents can play.

Australia should not opt for a narrower and more inflexible approach than has been adopted under the GDPR. In addition, it should not be so quick to jettison existing rules that define the scope of permitted use and disclosure of information by reference to the purposes for which the information was collected. These rules have been a feature of the Privacy Act since it was first introduced and should not be hastily discarded.

3.5. No need for changes to control and security

The introduction of a mandatory deletion of personal information obligation, as raised by the ACCC in the DPI report[12], would create significant regulatory burden and is not required. Entities may only retain personal information where it is accurate and necessary, and are required to take reasonable steps to destroy or de-identify that information once it is no longer needed for any purpose for which the information may be used or disclosed under the APPs.

The imposition of any obligation to automatically delete personal information may not always be practical or even possible, particularly considering the suggestion that technical information should be treated as

[12] This is acknowledged by the ACCC in the DPI report, p.473.

personal information. Requiring network operators to routinely purge their networks of all technical information could also present operational risk if the information is needed for the proper functioning of those networks. Further, imposing an obligation to delete information may also create uncertainty for organisations who have legitimate reasons to retain what they have generated, such as to comply with other legal obligations (as is the case under the telco metadata retention regime) or in order to be able to effectively deal with and respond to customer queries and complaints. There are also cases where deletion of personal information of an individual would impact the accuracy or quality of personal information we hold about another individual, for example in the case of a joint account or transactions between individuals such as call records.

While we acknowledge that individuals ought to be able to access their personal information, this needs to be appropriately balanced against the difficulty for entities to retrieve the information and the meaningfulness of the data to the consumer. For instance, data may be highly technical in nature and/or located in archives or deep storage, which may not be particularly helpful to the consumer but very costly for the entity to compile.

We do not believe a right to erasure is required. APP 11 already requires entities to take reasonable steps to destroy or de-identify personal information it holds when no longer required for a permitted purpose under the APPs. Any proposal to introduce a new right should be designed in close consultation with businesses and other stakeholders to ensure it is appropriately balanced and includes appropriate exceptions, such as where it is impractical for technical reasons or where the information must be retained for legitimate operational purposes or to satisfy other legal obligations. Article 17 of GDPR seems pragmatic in this respect, by saying "only where it is no longer necessary for the purpose for which it was originally collected". Further detail can be found in our answer to consultation question 46 in Appendix 1 of this submission.

Note that in the context of healthcare and health data, the right to erasure may not be appropriate and may contradict other regulatory requirements relating to record keeping and medical/ professional indemnity in both the public and private sectors. We recommend specific consultation with relevant stakeholders on this point.

3.6. No need to introduce a direct right of action or statutory tort

The DPI report recommended that a direct right of action be introduced in order to provide individuals greater control over their personal information and to provide an additional incentive for APP entities to comply with their obligations under the Privacy Act.[13] We do not agree that a direct right of action is the best way to achieve these aims, and see a well-resourced OAIC as a more effective way of continuing to pursue the Privacy Act's objectives.

A direct right of action has the capacity to divert consumers from OAIC's complaint and investigative processes, which we believe are well-suited to complaints under the Privacy Act, and which already permit applications to the Federal Court of Australia by the OAIC and the consumer in appropriate circumstances.[14] (Consumers also have the option of lodging complaints with the Telecommunications

[13] Issues Paper, page 67.

[14] Individual complainants or the OAIC may apply to the Federal Court or Federal Circuit Court for an order enforcing a determination made by the Commissioner (s 55A, s 62 of the Privacy Act); individuals may apply directly to the Federal Court of Federal Circuit Court for an injunction against a person contravening the Privacy Act (s 80W and *Regulatory Powers (Standard*

Industry Ombudsman.) The OAIC offers consumers an affordable and relatively quick avenue to resolve alleged grievances. The average time for the OAIC to finalise each complaint received in the 2019 – 2020 financial year was 4.7 months.[15] By contrast the Federal Court of Australia, which manages a large and diverse case load, advises that the first case management hearing for a newly filed claim '*will usually occur within five weeks of filing* [a] *matter'* and that the date set for trial '*may be several months after* [the] *first case management hearing*.'[16] Following a hearing the judge may reserve a further amount of time to consider the evidence before handing down a judgment and inviting the parties to make submissions about orders before the matter is finalised.

In addition, court proceedings may not be justified for many privacy complaints given the low amounts at stake in most privacy-related matters. The OAIC's most recent annual report shows that where a privacy complaint results in compensation being paid, in a large majority of cases payments involved are less than $10,000.[17] The cost, both to the parties involved and the courts, of court proceedings for matters of that magnitude is arguably hard to justify.

The flexibility of the OAIC's conciliation process is desirable in the context of privacy disputes. The process may result in a range of remedies including compensation, changed procedures, staff training, and apologies. The OAIC can bring parties together quickly to explore whether simple yet effective remedies are capable of resolving a dispute. For example, an apology featured in nearly 9% of the privacy complaints managed by the OAIC in the previous financial year.[18] By contrast, litigation has the potential to entrench parties' positions as the longer, more adversarial nature of the court process plays out.

We do not agree that a direct right of action is necessary to encourage compliance considering more targeted incentives that have been foreshadowed. Significant increases to penalties for breaches of the Privacy Act are planned and it is proposed that the OAIC will receive expanded powers to further deter and deal with non-compliance.[19] These initiatives, along with sufficient resourcing for the OAIC, constitute strong incentives for APP entities to comply with the Privacy Act to the benefit of all consumers.

In contrast to the laws that would underpin a direct right of action, we acknowledge that there is currently no tortious right of action for a serious invasion of privacy. While we consider a statutory tort to be unnecessary, if there were to be a demonstrated need then we support the ALRC recommendation that the tort be confined to intentional or reckless invasions of privacy and should not extend to negligent

Provisions) Act 2014 (Cth) s 121); the Commissioner may apply to the Federal Court or Federal Circuit Court for an order that an entity pay a penalty for contravening a civil penalty provision (s 80U) including under s 13G which makes an entity liable for a civil penalty for either engaging in an act or practice that is a serious interference with the privacy of an individual or repeatedly engaging in an act or practice that is an interference with the privacy of one or more individuals.

15 Office of the Australian Information Commissioner, Annual Report 2019-20 (Report, 21 September 2020) p.12.

16 https://www.fedcourt.gov.au/going-to-court/i-am-a-party/court-processes/preparing-for-court

17 Office of the Australian Information Commissioner, Annual Report 2019-20 (Report, 21 September 2020) p.135.

18 Ibid.

19 Increases to penalties are planned, from the current maximum penalty of $2.1 million for serious or repeated breaches to $10 million or three times the value of any benefit obtained through the misuse of information or 10 per cent of a company's annual domestic turnover (whichever is the greater); the OAIC is likely to receive expanded powers to issue infringement notices backed by new penalties and to publish prominent notices about specific breaches.
Source: Attorney-General's Department, **Tougher penalties to keep Australians safe online**
https://www.attorneygeneral.gov.au/media/media-releases/tougher-penalties-keep-australians-safe-online-24-march-2019

invasions or attract strict liability, as '[c]*onfining the tort in this way will ensure that the new tort applies to the most objectionable types of invasion of privacy*.'[20]

04 Consultation is required if changes are to be made

In this final section, we observe that if the AGD is of a mind to make changes to the Privacy Act, consultation is required.

4.1. Cross-border data flows and GDPR adequacy

One question posed by the AGD is whether Australia would be served by seeking adequacy under the GDPR. Only 12 countries have been granted adequacy by the European Commission;[21] the process made complex by the thorough analysis of how the applicant country's privacy regime must be amended to provide protections equivalent to those in the GDPR.[22]

In general, we support regulation designed to facilitate the global secure free-flow of data across borders. We also support increased global regulatory consistency when it comes to privacy and cross-border data flows. However, we consider that consumers would be better served by amendments made to the Privacy Act that are designed with Australia's unique regulatory, legal and cultural context in mind – rather than amendments made solely to achieve GDPR adequacy.

In any event, there are many open questions regarding what seeking GDPR adequacy would entail. We refer to this in answer to consultation questions 50 and 52 in Appendix 1 to the extent that seeking GDPR adequacy would require, for example, amendment to the definition of "consent". If the Government is serious about pursuing GDPR adequacy, Telstra requests further consultation and additional information on what the Government considers adequacy would entail.

4.2. Overlapping regulation

As the Issues Paper notes, there is a raft of different Commonwealth legislation which govern different types of personal information on top of the Privacy Act. This can lead to confusion both from a consumer perspective but also from a business perspective as they seek to comply with the different pieces of legislation. We strongly recommend a holistic review be undertaken on all these laws to ensure consistency and remove overlapping laws, where possible.

The Privacy Act already allows for different levels of protections for ordinary personal information compared to sensitive personal information. If there are other categories of information which, by their nature may attract additional risks, they should be covered under the framework of the existing Privacy Act. Having different levels of privacy protection for similar data, such as has been created in the

---

20 ALRC, Serious Invasions of Privacy in the Digital Era, ALRC Final Report 123, 2014, p.109.

21 European Commission, "Adequacy Decisions: How the EU determines if a non-EU country has an adequate level of data protection" (2020), available online at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

22 For Japan, that process took almost two years: see IAPP, "Japan's long road for adequacy under the GDPR" (2018), available online at https://iapp.org/news/a/japans-long-road-for-adequacy-under-the-gdpr

consumer data right (CDR) datasets and some telecommunications data covered by Part 13 of the Telecommunications Act 1997, creates unnecessary complexity and confusion.

It would also be beneficial to also consider harmonisation with State and Territory laws that deal with personal information including, for instance, surveillance device laws, as well as privacy and health data records laws. Most individuals would expect the level of protection afforded to their personal information to be the same nationally. Again, this harmonisation will make it easier for businesses to comply and for individuals to better understand their rights so they can exercise them. Alignment across jurisdictions would also provide wide ranging benefits including for industry as suppliers of systems that design and manage controls for these data across jurisdictions.

Appendix 1: Answer to questions in the consultation

This appendix contains answers to some of the questions raised in the issues paper.

Objectives of the Privacy Act

1. Should the objects outlined in section 2A of the Act be changed? If so, what changes should be made and why?

We consider there is no need to change the objects of the Act, as they are still relevant, applicable and fit-for-purpose. Specifically, we believe there is no need to remove or adjust the second object of the Act (recognising that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities) as we believe it necessary to strike an appropriate balance between customer interests and legitimate business activities, as well as evolving data use practices.

The protection of individuals' privacy is not incompatible with the interests of businesses. Allowing a business to operate efficiently and effectively can lead to real benefit for the consumer by way of innovation and offerings better tailored to meet their needs. At the same time, it is in the interests of businesses to appropriately protect the privacy of their customers to both retain and grow their customer base.

We support the existing objectives of the *Privacy Act 1988* (Cth) (**Privacy Act**), which strike this balance in a technology-neutral, principled way. Further expansion on our view can be found in section 2.1 in the body of this submission.

Definition of personal information

2. What approaches should be considered to ensure the Act protects an appropriate range of technical information?

The existing definition should be retained and does not need to be updated to provide appropriate protection for technical information.

To the extent technical information reveals something about an individual and the individual is reasonably identifiable, then it will be caught by the current definition. If it does not, then there is no privacy-related justification for giving that information special protection.

The Courts are quite capable of assessing whether there is sufficient connection between the information and the individual to justify this level of protection. In the Grubb case, the Full Federal Court found that:

> *The words "about an individual" direct attention to the need for the individual to be a subject matter of the information or opinion. This requirement might not be difficult to satisfy. … However, in every case it is necessary to consider whether each item of personal information requested, individually or in combination with other items, is about an individual. This will require an evaluative conclusion, depending upon the facts of any individual case, just as a determination of whether the identity can reasonably be ascertained will require an evaluative conclusion.*

4. Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?

We do not consider that additional protections are required. De-identified/anonymised/pseudonymised information should no longer be regarded as personal information (as there is nothing capable of linking it back to a natural person) and, therefore, it ceases to fall under the regulation of the Privacy Act. We note the OAIC already provides guidance on what constitutes de-identified or anonymised information[23] and we consider an appropriate solution, should further clarification or guidance be required would be to update this guidance.

See also section 3.2 for further expansion of our views on de-identified, anonymised and pseudonymised information.

Notice of Collection of Personal Information

23. Where an entity collects an individual's personal information and is unable to notify the individual of the collection, should additional requirements or limitations be placed on the use or disclosure of that information?

As stated in section 3.3 above, it is not uncommon for organisations to engage specialist contractors to assist them with their business operations so they can provide services to their customers, for example, printing houses to print customer bills or IT helpdesks to help resolve customer IT complaints. Limiting the use or disclosure of information in these situations would have a negative effect on businesses and lead to operational inefficiencies. Alternatively, requiring separate notification in these circumstances when the purpose for which the personal information is being used has not materially changed, would lead to regulatory burden without significant benefit to consumers. It would also risk consumers getting "notification" fatigue from receiving multiple notices for essentially the same use by or on behalf of the same organisation and could lead to an increased sharing of consumer contact personal information so these entities can send notices (even if they didn't need that information to provide the specialist services).

There are also legitimate circumstances when an APP entity may receive personal information of an individual indirectly. The most common is that of authorised representatives on an account. The APP entity would normally only need a small amount of personal information for that purpose. If the ACCC's recommendation from the DPI Report was implemented, the APP entity would need to obtain full contact details of that representative to send them a notice.

The focus of any reforms is this area should be on ensuring that notices are only provided where are meaningful (i.e. where there is a change that may legitimately lead a consumer to change their behaviour).

[23] OAIC Guide on De-identification and the Privacy Act, available at: https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act This guide is helpfully complemented by the De-identification Decision-Making Framework, jointly developed with CSIRO's Data61, available at https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-decision-making-framework/

Consent to collection and use and disclosure of personal information

28. Should individuals be required to separately consent to each purpose for which an entity collects, uses and discloses information? What would be the benefits or disadvantages of requiring individual consents for each primary purpose?

If there is the ability to erase/delete data, then entry & Consent is less important, because you can always leave and have your data deleted.

Consent for each collection, use or disclosure will be burdensome for both organisations and consumers. Not in the interest of customers.

Need to be clear what is "necessary for the performance of contract" vs things which are a necessary incidental eg: in addition to providing customer service, we need to be able to detect fraud, protect our network so we can provide service, improve network and service, compliance with law etc.

Requiring that consents be unbundled is consistent with the proposition that they should be both voluntary and specific. However, without other valid legal bases for processing information besides consent, it is also likely to result in consumers being swamped with requests for consent. That will not necessarily drive meaningful engagement by consumers on privacy-related issues and, therefore, will not necessarily be good for consumers.

A better approach would be to retain consent as just one of a number of equally legitimate legal bases for processing personal information, perhaps with a special role to play in relation to higher sensitivity processing activities (e.g. in relation to collection and use of health or other sensitive information, as is currently the case). This is consistent with the GDPR, which provides for "legitimate interests" as a lawful basis for processing personal data, alongside consent and other lawful bases. In this case, requiring that consents be unbundled in order to be valid would make sense and would reflect the special role that consents can play.

Australia should not opt for a narrower and more inflexible approach than has been adopted under the GDPR. In addition, it should not be so quick to jettison existing rules that define the scope of permitted use and disclosure of information by reference to the purposes for which the information was collected. These rules have been a feature of the Privacy Act since it was first introduced and should not be hastily discarded.

34. How can the personal information of individuals be protected where IoT devices collect personal information from multiple individuals?

The challenges identified in relation to IoT devices serve to illustrate the practical risks associated with reforms that would over-emphasise the role of consent, in particular the risk that such a regime would deter innovation and limit the introduction or expansion of new technologies that may be beneficial for consumers. For this reason, it is important to have legal bases for processing personal information other than consent.

Control and security of personal information

44. Should there be greater requirements placed on entities to destroy or de-identify personal information that they hold?

We propose there is no need to change the Act to introduce new requirements to destroy or de-identify personal information. There is already an obligation under the Act to either de-identify or delete data for which there is no longer a legitimate business purpose. Once this is done, it is no longer PI, and therefore falls outside the Act.

Further, any such obligation may not always be practical or even possible, particularly considering the suggestion that technical information should be treated as personal information. Requiring network operators to routinely purge their networks of all technical information could also present operational risk if the information is needed for the proper functioning of the networks.

Imposing an obligation to delete information may also create uncertainty for organisations who have legitimate reasons to retain what they have generated, such as to comply with other legal obligations (as is the case under the telco metadata retention regime, or in the health sector) or in order to be able to effectively deal with and respond to customer queries and complaints.

45a. Should amendments be made to the Act to enhance transparency to individuals about what personal information is being collected and used by entities?

We consider the APPs already provide for transparency as to how businesses collect and use personal information. APP1 covering Open and transparent management of personal information, including ensuring that businesses manage personal information in an open and transparent way, including having a clearly expressed and up to date privacy policy. APP5 also outlines when and in what circumstances a business must tell an individual about certain matters related to their personal information.

In our view, given these obligations already exist, should individuals require further clarification or guidance on what personal information is being collected or used by entities, we propose it would be better to update the guidance that accompanies these principles to provide clarity, rather than amending the Privacy Act to provide the clarification. Updating supporting information such as accompanying guidance is an appropriate mechanism, as it can be updated again in the future as technology evolves further.

We expand on this further in section 3.3 in the body of our submission.

46. Should a 'right to erasure' be introduced into the Act? If so, what should be the key features of such a right? What would be the financial impact on entities?

We do not believe a right to erasure is required, given APP 11 already requires that where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that it is de-identified. If the OAIC plans to consider introducing a right to erasure, we recommend a careful analysis of requirements, technical impediments/considerations, costs and benefits is performed. To highlight just two potential impediments we foresee, we consider:

- It can be impractical for technical reasons to delete information, such as where the information is not readily accessible (e.g. in the case of network metadata because it is dispersed across multiple network elements), especially where the information will in the ordinary course be deleted according to a regular cycle (e.g. where networks are configured to retain metadata for a defined period that is not excessive); and
- Information must be retained for legitimate operational purposes or to satisfy other legal obligations. For example, in the telecommunications context, there are specific obligations for carriers and carriage service providers to retain certain categories of network metadata, which are already deemed to be "personal information" for the purposes of the Privacy Act, for a minimum period of 2 years.

Any new right should also be designed in close consultation with businesses, given that experience in the EU in relation to the GDPR "right to be forgotten" suggests that there may be significant work and costs involved in developing suitable compliance systems. Article 17 of GDPR seems more pragmatic in this respect, by saying "*only where it is no longer necessary for the purpose for which it was originally collected*".

In the context of healthcare and health data, the right to erasure may not be appropriate and may contradict other regulatory requirements relating to record keeping and medical/ professional indemnity in both the public and private sectors. We recommend specific consultation with relevant stakeholders on this point.

Overseas data flows and third-party certification

50. What (if any) are the challenges of implementing the CBPR system in Australia?

Particularly after the CJEU's recent decision in *Data Protection Commissioner v Facebook Ireland Ltd* ("Schrems II"), there is divergence globally regarding the circumstances in which cross-border data flows are permitted. Uncertainty and inconsistent regimes increase the regulatory burden on companies operating in multiple jurisdictions. Australia should participate in the ongoing global debates (including those at the OECD) before taking decisive action implementing a CBPR system/certification scheme, with the aim of encouraging more global regulatory consistency.

Should Australia decide to implement a CBPR system, that system should be voluntary to minimise regulatory compliance complexities for companies that would not be served by such a system. Any CBPR system should also be aligned with the requirements of the Privacy Act to ensure a consistent approach to privacy in Australia.

52. What would be the benefits or disadvantages of Australia seeking adequacy under the GDPR?

The obvious benefit of Australia seeking adequacy under the GDPR is that it would facilitate free flow of personal data across these jurisdictions. However, the decision to seek adequacy should not be taken lightly. Aligning Australia's privacy regime such that it offers protections 'essentially equivalent'[24] to the GDPR would not necessarily result in reform best suited to Australia's unique legislative and regulatory environment and privacy culture. Although Telstra is supportive of the secure free flow of data across

[24] GDPR, Recital 104. See also GDPR, Art. 45.

borders, Telstra requests that the AGD engage in thorough public consultation before pursuing this course of action.

Direct right of action

56. How should any direct right of action under the Act be framed so as to give individuals greater control over their personal information and provide additional incentive for APP entities to comply with their obligations while balancing the need to appropriately direct court resources?

As explored in section 3.6 of our submission, we do not agree that a direct right of action is the best way to provide consumers with greater control over their personal information or to incentivise compliance. We see a well-resourced OAIC as a more effective way of continuing to pursue the Privacy Act's objectives.

A direct right of action will offer individuals another avenue via the Federal Courts to seek to enforce their rights, but that avenue is likely to be more drawn-out, costly, and less flexible than the current complaints process offered by the OAIC. In contrast, the OAIC is a specialist body that can finalise complaints relatively quickly and cheaply for consumers and facilitate a range of remedies. Even if a small proportion of complaints are diverted away from the OAIC as a first port of call then that could result in a significant imposition on court resources, which is likely to be unjustified in light of the monetary awards under consideration – the OAIC's most recent annual report shows that only a small proportion of privacy complaints result in compensation, and where compensation is paid in most cases it is less than $10,000.

Determinations made by the OAIC are made public and can subsequently be enforced through the courts, and so carry suitable weight. Individuals already have the power to apply to the courts for an injunction to restrain a breach of their privacy, which may be the appropriate course in urgent matters of non-compliance. In these circumstances, it is not necessarily clear that there is a need for individuals to have a direct right of action.

In section 3.6 we also highlighted that there are more effective ways to incentivise APP entities to comply with their obligations. The planned increases to civil penalties under the Privacy Act, as well as an expansion of the OAIC's powers, are more targeted measures for ensuring compliance. The OAIC has demonstrated by commencing its first civil penalty action in 2020 that it will not shy away from prosecuting APP entities for alleged serious non-compliance.

Interaction between the Act and other regulatory schemes

66. Should there continue to be separate privacy protections to address specific privacy risks and concerns?

The Privacy Act already allows for different levels of protections for ordinary personal information versus sensitive personal information. If there are other categories of information which, by their nature may attract additional risks, this should be able to be covered under the framework of the existing Privacy Act. Having different levels of privacy protection for similar data (such as under the consumer data right (CDR) datasets and some telecommunications data covered by Part 13 of the Telecommunications Act 1997) adds to unnecessary complexity and confusion. We would strongly recommend a holistic review be undertaken on all these laws to ensure consistency and remove overlapping laws, where possible.

Further details are contained in section 4.2 in the body of our submission.