SERVICES AUSTRALIA

28 January 2022

PRIVACY ACT REVIEW DISCUSSION PAPER: SERVICES AUSTRALIA'S SUBMISSION

OFFICIAL

Australian Government

Services Australia

Contents

Introduction

Services Australia (the Agency) welcomes the opportunity to make a submission on the review of the *Privacy Act 1988* (Cth) (Privacy Act) currently being undertaken by the Attorney-General's Department.

This submission encompasses the Agency's views in relation to the Discussion Paper distributed by the Attorney-General's Department. In preparing this submission we have consulted with key internal business areas within the Agency and relevant external policy departments (Department of Social Services (**DSS**), Department of Health and the National Recovery and Resilience Agency).

The last major reform of the Privacy Act occurred in 2014 with the introduction of the Australian Privacy Principles (**APPs**). The last 7 years has seen the data and technology landscape change significantly with advances in technology and the move to use different types of personal information, such as biometrics, to enable more customised services to be provided to individuals.

In that time, the Agency has embarked on a major transformation program to overhaul Australia's welfare payment system, and to introduce scalable online platforms that can be re-used across government and can enable streamlined, more personalised and timely services to customers.

Services Australia's vision is, 'to make government services simple so people can get on with their lives'. Services Australia handles vast amounts of personal information about almost every person in Australia, as part of its various roles as:

- a consumer of personal information in order to design, develop, deliver, coordinate and monitor government services and payments relating to social security, child support, students, families, pensions, aged care and health programs;
- a consumer of personal information for the purposes of providing customer service functions on behalf of other Commonwealth Government agencies such as the Department of Home Affairs and the Department of Health (and state and territory government agencies when required);
- an ICT services provider for the Commonwealth Government, handling personal information on behalf of other government agencies through the provision of whole of government platforms such as myGov and Payment Utility and providing ICT services for other Commonwealth Government agencies, such as the Department of Veterans' Affairs and the National Disability Insurance Agency; and
- an employer.

Proposal 1: Objects of the Act

The Agency notes the proposal to amend the objects of the Act in section 2A to clarify the Act's scope and to introduce the concept of public interest (to recognise that the protection of the privacy of individuals must be balanced with the interest of entities in carrying out their functions or activities which are undertaken in the public interest). Services Australia has no further comment on the proposed change noting that it has in place robust privacy practices and project management frameworks, to manage the public interest aspect of its work and activities.

Proposal 2: Personal information, de-identification and sensitive information

Broadening the definition of personal information

The proposal to amend the definition of 'personal information' is intended to address uncertainty about how this definition applies to technical and inferred information. It is important that the definition of 'personal information' is clear enough to provide APP entities, and the public with confidence about the protections under the Act.

We support the desire for certainty. However, changing the definition of 'personal information' in the Privacy Act by removing the word 'about' and replacing it with the words 'relates to' would potentially create an extremely broad definition and could create unanticipated consequences.

The phrase 'relates to' means there must be a connection between the individual and the information, but it is unclear how strong that connection needs to be. If the definition of 'personal information' is to be expanded, then clear and detailed guidance on the required connection with the information is needed.

In terms of technical information, it is not clear why IP addresses are proposed to be specifically reclassified as 'personal information'. We note that if IP addresses are capable of identifying an individual they would already be personal information. If IP addresses are to be explicitly classified as 'personal information' careful consideration should be given to guidance to ensure privacy compliance is not administratively burdensome for agencies (including with respect to fraud and compliance activities).

Another example of the need for clear guidance would be cookies. Would all types of cookies be caught by the expanded definition of 'personal information' (noting there are different types of cookies that achieve different things)?

The Discussion paper raises some key questions:

- whether the definition of 'sensitive information' should be updated to maximise interoperability with international frameworks.
- the sensitivity of location information, given the increasing ability for digital platforms to track individuals' locations
- the sensitivity of financial information, given sensitive information is readily inferred from financial data.

'Sensitive information', has a higher level of privacy protection afforded to it under the Act, for

instance, the requirement for consent to be provided on collection.

The inclusion of new types of information in the definition of 'sensitive information' would impact on the operations of agencies. For example, unique identifiers, which have been created to identify the correct record for an individual without identifying the individual themselves may come within the proposed definition of personal information. This could impede the efficient administration of some programmes.

Requirement for information to be anonymised

The proposal to lift the threshold (for information not to be covered by the Privacy Act) to anonymisation, so as to protect against the risk of re-identification, combined with the proposed broadened definition of personal information is likely to impact on the ability to conduct research projects and customer journey analytics activities. Such activities inform the design of services to ensure they are accessible and customer focused.

This change is likely to have a significant impact on how/what data can be collected, stored, retained and referred back to as audit evidence if the information needs to be 'anonymous' rather than 'de-identified'. Given the conditions to meet the definition of 'anonymous', identifiers that can lead to an individual will need to be removed in a way that means they are not capable of being identified.

This will require significant changes to ICT systems and controls around receiving customer information where the current requirement is for de-identified information only. Systems are currently built on the assumption that such identifiers are not personal information.

The requirement for anonymisation may create uncertainty and will likely involve significant regulatory burdens, inefficiency and cost to all entities.

Broadening the definition of 'sensitive information'

Including financial information in the definition of sensitive information would increase regulatory requirements, requiring the collection of consent from employees for everyday tasks, such as paying wages and reimbursing expenses.

It would also likely affect related secondary uses and disclosures. Government agencies handle vast amounts of financial information in the context of processing claims and making payments to eligible individuals. Financial information such as bank details, are disclosed to the RBA to ensure eligible recipients receive their payments.

Financial information is also used for compliance activities. Such activities may involve the disclosure of financial information in accordance with APP 6.2(b). Should the definition of sensitive information be expanded to include this type of information, it is important that clear exceptions are provided where consent is not appropriate (for instance, where there is fraud and potential or actual criminal activity being investigated).

Location data may be used to confirm eligibility for emergency payments. The proposals in relation to location data should be scoped with this context (emergency responses) in mind. If location data is to be included in the definition of sensitive information, consideration should be given to an exception to the requirement to obtain consent to collect, use or disclose location data in circumstances where the collection, use or disclosure is in response to a emergency, natural disaster or other crisis where the individual may not be at imminent risk of serious harm but is unable to comply with the administrative processes required. An exception for fraud and potential or actual criminal activity should also be provided.

The term 'location data' is potentially broad and will need to be clearly defined.

Broadening the definition of 'collection' to cover inferred information

The proposal is to amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred and generated information.

Expanding the definition would require extensive changes to infrastructure, systems and processes, including in relation to the administration of the whole of government platforms.

It may also require the tagging of information, to monitor where the data was collected from and under what circumstances (i.e. under what legislation if any) to determine for which purposes it can be used. This would be a significant exercise and likely not achievable for information collected to date and so should not apply retrospectively.

We recommend APP entities are provided with sufficient lead time to enable changes to systems, infrastructure and processes. There is significant concern about the time needed and the cost to make the necessary changes required under proposal 2. Large organisations with complex systems typically require significant lead times to implement wholesale ICT changes.

Recommendations for Proposal 2:

- In relation to the definition of personal information, any legislative change will need to ensure clarity about:
    - The strength of the connection required between the individual and the information to bring that information within its scope; and
    - How APP entities are to meet the new 'anonymous' standard in order for the Privacy Act not to apply.
- If financial information is to be included within the definition of sensitive information, consideration should be given to including an exception to the requirement to obtain consent for certain activities where it is impractical to do so (e.g. for payroll and human resources functions, for potential or actual fraud, criminal or other related activities or purposes);
- If location data is to be included in the definition of sensitive information, consideration should be given to an exception to the requirement to obtain consent where this occurs in response to a natural disaster, or other crisis where the individual may not be at imminent risk of serious harm, but is unable to comply with the administrative processes required. An exception may also be needed for potential or actual fraud and criminal activities;
- A clear definition of 'location data' should be included in the Privacy Act if specific reference is to be made to it.
- Entities need sufficient lead time to enable changes to systems, infrastructure and processes.

Proposal 3: Flexibility of APPs

In relation to proposal 3.3 on Emergency Declarations, we note that specificity with regard to the drafting of Emergency Declarations needs to be balanced with the flexibility required to meet the needs of the community during times of crisis such as natural disasters.

Recommendation for Proposal 3: Balance the need for specificity in Emergency Declarations with the need for flexibility to enable entities to be able to meet the needs of the community during times of crisis.

Proposal 8: Notice of Collection of Personal Information

In relation to proposals regarding APP 5, to standardise privacy notices and to strengthen the requirements for when collection notices are required, it is important that notices be targeted for the circumstances and purpose they serve. Notice requirements must be flexible enough to ensure consent can be collected and individuals notified at appropriate times; but must also recognise that it is not always possible to provide notice to individuals.

For instance, where an APP entity receives tip-offs of alleged fraud by or about individuals, information about alleged perpetrators of child abuse or neglect, details of domestic and other violence and other matters concerning the mistreatment of vulnerable persons, or criminal or fraudulent activities, exceptions to notice requirements would clearly be necessary.

Recommendation for Proposal 8: Any notice requirements must be flexible enough to ensure we can collect consent at appropriate times and notify individuals at suitable times, but also recognise that it is not always possible to provide notice to individuals.

Proposal 9: Consent to the collection, use and disclosure of personal information

Proposal 9.1 is that consent be defined in the Act as being voluntary, informed, current, specific and an unambiguous indication through clear action. This infers a need to obtain refreshed consent.

It will be important to ensure that the requirement to refresh is not too onerous or required too often, so that individuals do not become 'consent fatigued' or treat this as 'a tick a box' exercise; and that exceptions are made for certain cohorts such as individuals who have an enduring power of attorney.

The proposed requirement for valid consent has implications for different sectors, such as healthcare, in relation to consent of a minor (discussed below under 'Children and capacity to consent').

Recommendations for Proposal 9:

If requiring APP entities to refresh or renew consent, this requirement should not be too onerous and should be balanced against issues such as consent fatigue.

Proposal 10: Additional protections for collection, use and disclosure

Proposal 10 is to include an additional requirement under APP 3.6 to the effect that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3. This could have unintended consequences. Personal information as defined, is not always originally collected from the individual to whom it relates; it could be created by an entity from which Services Australia collects information.

For example, payroll and employment information which may be considered sensitive information if the definition is expanded to include financial information is collected by Services Australia from the Australian Taxation Office (**ATO**). The ATO collect such information about its customers from employers who create that information. This information is collected in accordance with legislation administered by the Department of Social Services. An exception for collections, uses, and disclosures that are authorised or required under an Australian law, should be included.

A fair and reasonable test would seem appropriate across collection, use and disclosures (APP 3 and 6), as long as the exceptions and permitted general situations remain unchanged, as these are often relied on for secondary uses and disclosures by APP entities (for example, the law enforcement exception).

In relation to this proposal in the context of personal information related to a child, we support a requirement to consider what is in the best interests of the child. In practice it is unclear how this can be met where the dealings with personal information are entirely in the online space and the organisation has no direct relationship with the child. Considerations of the best interests of the child appear to require a subjective consideration of what is in the particular child's best interests in the circumstances, and assumes a level of understanding of that child's situation. This would be a very challenging requirement, if possible at all. If this proposal were to progress, there would need to be detailed and clear guidance on how entities are to meet such a requirement.

Regarding what is fair and reasonable, it would be helpful to maintain consistent requirements across the APPs in relation to collection, use and disclosure. The 'fair and reasonable' requirement would achieve the same outcome as the current requirements under APP 3.5 for collection of personal information to be fair and lawful. A collection that is fair and reasonable would essentially be one that is lawful.

In relation to the exceptions contained in APP 3.4, APP 6.2(a) and APP 6.2(b)-(f), these exceptions are necessary to provide flexibility in the lawful management of personal information. The particular exceptions are:

- the authorised or required by Australia law (APP 6.2(b)) exception;

- the permitted general situation exception (APP 6.2(c)); and
- the law enforcement (APP 6.2(e)) exception.

If a collection, use or disclosure is fair and reasonable to begin with, it will follow that any subsequent use or disclosure for a secondary purpose authorised under the exceptions is likely to be fair and reasonable. As such, there is no need to amend the exceptions contained in APP 3.4, APP 6.2(a) and APP 6.2(b)-(f). Amending those exceptions would create more red tape for no real benefit to include a fair and reasonable requirement. The exceptions should be maintained in their current form.

As to the proposed definition of a secondary purpose, this would inadvertently restrict socially beneficial uses and disclosures of personal information, such as public interest research. If all secondary purposes were known at the time of collection of the information, then it would be a primary purpose for collection and the individual would be able to be advised up front. However, as projects and uses expand and become known, new purposes for uses and disclosures that can be related or directly related to a primary purpose, become apparent. Identifying all secondary uses up front is a restrictive requirement.

A requirement for an entity to know where information was originally collected from and for what purposes, essentially requires tagging of all data. It will be important to ensure that requirement did not apply retrospectively.

For example, customer bank details are used to pay welfare payments, pensions and benefits to customers. In order to facilitate the payments, these details are shared with the Reserve Bank of Australia. If financial information becomes sensitive information and requires customer consent for disclosures, this would increase red tape and potentially impede service delivery. If the 'required or authorised by or under an Australian law' exception is maintained, this may support such disclosures without explicit need for consent.

It is important that the exception for criminal investigations to collect and use financial information to support offences against the Criminal Code, Social Security, Medicare and Child Support Acts continues. Government agencies have wide-ranging powers to obtain financial information or require documents to be produced that are relevant to administrative decisions made under enabling legislation.

For example, the following enabling Acts each contain a “general power to obtain information” as follows:

- section 192, *Social Security (Administration) Act 1999*
- section 154, *A New Tax System (Family Assistance) (Administration) Act 1999*
- section 343, *Students Assistance Act 1973*
- section 117, *Paid Parental Leave Act 2010*.

The delivery of the criminal investigation capabilities in the Commonwealth protects public money. This necessarily involves referrals to the Commonwealth Director of Public Prosecutions. Without the exemption for criminal investigations to collect and use financial information to support offences, such prosecutions would not be possible. That is, a requirement to become overt with the notification to suspected offenders or organised criminal syndicates would impact the ability to pursue criminal charges for referral for prosecution.

In relation to the proposal for the assumed age of capacity being 16 years in the Online Privacy Bill applying to all APP entities, as discussed below, further consideration is needed of the scope of parental consent required, and whether there are certain situations in which a requirement for parental consent would not be inappropriate.

Recommendations for Proposal 10:

- If the proposal to require collections, uses and disclosures of personal information to be fair and reasonable includes a requirement to consider the best interests of the child (when the personal information relates to a child), detailed and clear guidance will be required on how entities are to meet this requirement.
- The requirement to consider the factors of a fair and reasonable test should allow flexibility in the consideration of those factors (rather than mandating the consideration of all the factors) to enable decision-making that is appropriate to the circumstances;
- If a collection, use or disclosure is fair and reasonable to begin with, there is no need to amend the exceptions contained in APP 3.4, APP 6.2(a) and APP 6.2(b)-(f), as it would cause more red tape for no real benefit.

Proposal 13: Children and capacity to consent

The proposal is for the assumed age of capacity to be 16 years and this apply to all APP entities. Further consideration is needed of the scope of parental consent required, and whether there are certain situations in which a requirement for parental consent would not be appropriate.

The protection of the privacy of young people is important, particularly as it relates to ensuring safety and encouraging access to important services and interventions.

Various health programmes administered on behalf of the Department of Health including Medicare, the Pharmaceutical Benefits Scheme, the Australian Immunisation Register, Australian Organ Donor Register and the National Cancer Screening Register involve the collection of information about customers and service providers, for example to pay benefits for Medicare (and the Medicare Safety Net), and the Pharmaceutical Benefits Scheme.

Health information is also collected under the My Health Records service.

The issue of minors and consent is a complex one and making changes without proper consideration could have unintended consequences and result in inconsistencies in the rules that apply, specifically in relation to capacity to consent. Among other considerations, we note the following matters would need to be considered:

- Medicare policy which enables minors 14 years and above to handle their own health information exclusively;
- Privacy Act presumption of capacity from 15 years (as set out in the APP guidelines);
- *My Health Record Act 2012* requiring a child to authorise a representative if they so choose from 14 years and above;
- persons aged 16 years and over can register their donation decision on the Australian Organ Donor Register. It is Government policy that family consent is required for all persons on the register before donation can proceed. Persons under the age of 16 years cannot be registered on the Australian Organ Donor Register. The family's decision and consent is required for organ donation and/or tissue transplantation to proceed; and

- the Online Privacy Code which, should it come into effect, will contain provisions creating a presumption that minors under 16 years of age will not have capacity to consent.

As the position stands, 14 year olds with capacity can make their own decision regarding their personal health. It would be inconsistent with that position to overlay a requirement that parental consent to the disclosure of these individual's health information be required.

The above matters create a complex framework in relation to minors and capacity to consent In addition, the proposal does not consider circumstances where parental consent may not be possible, (for instance, an orphan who is living independently).

Recommendations for Proposal 13:

- Consideration should be given to driving consistency between legislative requirements and various health policies in relation to the treatment of minors and consent to the handling of their health information;
- Consideration should be given to the inclusion of an exception for orphan children and children who are living independently of the need for parental consent;
- APP entities will need sufficient time to assess the potential impact of the proposed changes, including cost and implementation timeframes.

Proposal 15: Right to erasure

With respect to the proposal to introduce a right to request erasure on certain grounds, reasonable exceptions should apply for some requests, such as, fraud and law enforcement activities.

Proposal 22: Overseas data flows

The Discussion Paper asks, "Would the other exceptions to APP 8.2, together with proposals such as creating a list of prescribed countries and binding schemes, and introducing standard contractual clauses, facilitate overseas disclosures of personal information in the absence of the informed consent exception?"

We consider this would be a positive improvement if the privacy regulator were to maintain this list as it would facilitate APP entities to be able to share information where appropriate; and would enable individuals to make better informed decisions about whether to provide consent to such disclosure.

servicesaustralia.gov.au

Australian Government

Services Australia