Privacy108
PO Box 3295
Yeronga, QLD 4105

29 November 2020
Attorney-General's Department
4 National Circuit
BARTON ACT 2600
By email: PrivacyActReview@ag.gov.au

Dear Attorney-General,

RE: Review of the Privacy Act 1988

Thank you for the opportunity to make submissions in relation to the review of the Privacy Act 1988. Please find our submission attached. We have no objection to the publication of this submission.

Please let us know if we can provide any clarification about our response.

Thank you for your consideration.

Yours sincerely,

Dr Jodie Siganto CISSP, CISM, CIPM, CIPPE, CIPT

Mobile +61 (0) 408 275 733
Email jodie.siganto@privacy108.com.au
Web www.privacy108.com.au

Privacy108
We Protect Privacy

Response to Review of the Privacy Act – 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 are strongly against any change to the objectives of the Privacy Act that would place a greater emphasis on protecting consumers or on the principle that consumers are sufficiently protected by the ability to make informed choices, outside the other protections on collection and use.

As discussed further below, the Privacy Act was never intended and should not be modified to act as a form of consumer protection. As the recital says, the Privacy Act implements our international obligations in relation to privacy arising out of human rights and is not and should not be re-cast as a form of consumer protection.

While the ACCC has an important role to play in protecting consumers form unfair and deceptive conduct and from the predatory behaviour of organisations with market power, these powers should be used in conjunction to the principles established by first and second generation privacy laws likes those included in the Privacy Act.

If amendment is to be made to the objectives, it would be to embed the concept of the importance of the protection of privacy as a fundamental human right.

We would also support any change that reflect the idea of fairness and ethical decision making in regard to data, balancing the rights of individuals against those of regulated entities.

Definition of personal information

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

The definition of 'personal information' is fundamental to the operation of the Act and we strongly are of the view that care be taken in any overly prescriptive amendment.
Generally, we support the operation of the Act as a principle based regulatory system, supported by guidance and education from the regulator. Consistently with the principle-based regulatory approach in the Privacy Act, we do not support any amendment which will introduce more prescriptive or technologically specific provisions.

However, given the current jurisprudence (and lack thereof) as to the interpretation of the term 'personal information' and the more mature definitions used in second-generation privacy laws we recommend:

- That the word "about" be changed to "which relates to"; and

- That the reference to an "identified individual, or an individual who is reasonably identifiable" be changed "identified or identifiable individual."

These amendments would make the definition more consistent with that of other jurisdictions and reduce issues caused by varying definitions and conflicts around the application of the Act in the context of privacy laws.

3	***Should the definition of personal information be updated to expressly include inferred personal information?***

We recommend that inferred personal information be included by way of note or guidance rather than by change to the definition itself.

We believe that the term 'identifiable' should be interpreted to include the ability to identify the existence of a unique individual without necessarily being able to identify that individual by name or contact details. It should also be expressly provided that the identifiability test is not considered in isolation. This would ensure that the term includes data drawn from the profiling or tracking of behaviours or movements (and all other data points aggregated as part of the move to surveillance capitalism). Any data that enables an individual to be singled out (i.e. disambiguated from a crowd or cohort) and thus subjected to targeting or intervention, even if the individual cannot be identified per se from the data, should be included.

Given the uses of inferred data, we submit any definition that require strict identification of the individual is no longer appropriate to provide the protections that most Australians would believe to be appropriate.

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

We submit that our interpretation of 'de-identification' should be made consistent with the GDPR and other jurisdictions.

We also support the formal recognition of the importance of pseudonymisation and data minimisation as important data protection techniques. It would be useful to clarify the intended meaning and application of the terms often used interchangeably in this context including de-identification, anonymisation, pseudonymisation and confidentialisation.

We further submit that this is an area where the OAIC could work more closely with the regulated community to establish more regularly updated expectations and guidance.

The work done by CSIRO Data 61 is excellent and should be more widely promoted. However, the OAIC Guidance for the privacy community on this topic (which refers to the CSIRO work) was published in 2018. In this constantly changing environment, where de-identification and pseudonymisation are foundational concepts for privacy technologists, more current guidance reflective of changing technologies and business uses would be useful.

5	***Are any other changes required to the Act to provide greater clarity around what information is 'personal information'?***

We believe that the Office of the Australian Information Commissioner (OAIC) should be more fully resourced to be able to produce more detailed and timely guidance around what information is 'personal information' (in addition to guidance around supporting concepts such as technical identifiers, inferred information and de-identification).

Principle based regulation only works where there is consensus between the regulator and regulated community as to the meaning of the principles. This is particularly important where considering a threshold concept such as our understanding of what is 'personal information.'

Flexibility of the APPs in regulating and protecting privacy

6	***Is the framework of the Act effective in providing flexibility to cater for a wide variety of entities, acts and practices, while ensuring sufficient clarity about protections and obligations?***

We submit that there would be significant benefit to the regulated community if a single privacy framework could be developed to apply to all Australian entities, including Federal and State government agencies.

We appreciate the issues with this approach but note:

- There are significant gaps in protection in those States which have not yet passed a comprehensive privacy law;
- The exemptions for contracted service providers to State agencies can result in entities having no privacy obligations at all in relation to the processing of data on behalf of State agencies.

We also note that the lack of consistency between Federal and State privacy regimes is confusing and significantly increases the compliance burdens particularly for not-for-profit organisations which deliver services across State borders.

We also submit that a system like that under the GDPR where there is a single legal regime but with separate enforcement authorities across the member states, operating under a combined board of regulators, could be a model that works for Australia. It would provide consistency but at the same time support local enforcement but as part of a system that worked to resolve any inter-State differences.

Exemptions

Small business exemption

7	***Does the small business exemption in its current form strike the right balance between protecting the privacy rights of individuals and avoid imposing unnecessary compliance costs on small business?***

We submit that the small business exemption should be deleted from the Act. While perhaps a relevant consideration 20 years ago when the Act was amended to extend to privacy entities, we believe that the exemption is no longer suitable for businesses in the modern economy.

Privacy108
We Protect Privacy

Many small businesses, particularly those on-line, collect signification amounts of personal data and Australians would expect that that data was properly protected. Many other small businesses do not collect large amount of personal data and their obligations will be commensurately reduced. One of the benefits of principle-based regulation is its flexibility of application. This is particularly important when considering the application of the privacy principles to small businesses. Their compliance burden is not affected by prescriptive requirements that apply regardless of size of the organisation but will be commensurate with the quantity and sensitivity of the personal they collect. From a practical perspective, we have also worked with small businesses outside the scope of the Act but covered by other legislation, such as the GDPR. Together we have been able to develop privacy protective practices that support the regulatory obligations of those organisations without a significant financial or resource impost.	
8	***Is the current threshold appropriately pitched or should the definition of small business be amended?*** ***a. If so, should it be amended by changing the annual turnover threshold from $3 million to another amount, replacing the threshold with another factor such as number of employees or value of assets or should the definition be amended in another way?***
As submitted above, we support the removal of the small business exemption from the Act.	
9	***Are there businesses or acts and practices that should or should not be covered by the small business exemption?***
As submitted above, we support the removal of the small business exemption from the Act.	
10	***Would it be appropriate for small businesses to be required to comply with some but not all of the APPs?*** ***a. If so, what obligations should be placed on small businesses?*** ***b. What would be the financial implications for small business?***
As submitted above, we support the removal of the small business exemption from the Act.	
11	***Would there be benefits to small business if they were required to comply with some or all of the APPs?***
As submitted above, we support the removal of the small business exemption from the Act.	
12	***Should small businesses that trade in personal information continue to be exempt from the Act if they have the consent of individuals to collect or disclose their personal information?***
As submitted above, we support the removal of the small business exemption from the Act.	
Employee records exemption	
13	***Is the personal information of employees adequately protected by the current scope of the employee records exemption?***
No.	

The basis for the exclusion of employee records is no longer valid. In particular, the protections available for employee records outside of the Act (e.g. under Fair Work legislation) is not sufficient and does not justify the exemption of employee records from the Act. The exemption leads to uncertainty, confusion and inconsistency of practice for international organisations. Within Australia, it is not obvious why the employee records of Federal government agencies should be protected while those of private entities are not.	
14	***If enhanced protections are required, how should concerns about employees' ability to freely consent to employers' collection of their personal information be addressed?***
The use of consent in relation to employers collection and use of personal information is a powerful example of the issues with relying on consent as the basis for processing. Not only is it difficult to establish in the context of the employer/employee relationship, there are many instances where the collection should not be allowed, regardless of how 'free' the consent is. We submit that this is an area where the OAIC could work more closely with other regulators to develop more guidance and support for employers. With the push for more privacy invasive technologies in the employment space (including for example the use of AI for performance management) this is an important area for future focs.	
15	***Should some but not all of the APPs apply to employee records, or certain types of employee records***?
We submit that the exemption of employee records should be removed from the Act. All of the APPs should apply to employee records.	
Political party exemption	
16	***Should political acts and practices continue to be exempted from the operation of some or all of the APPs?***
We submit that there is no basis for the exemption of political parties from the Privacy Act. There is no clear reason why the privacy principles should not operate in relation to the use of personal information by political parties. In fact, the significant increase in profiling and targeting of individuals for political messaging, that has become part of every political parties' standard tools for attracting support, makes it even more important that the privacy principles be extended. They should apply to the collection and use of personal data by political parties. Again, this is an area where the OAIC could work on the development of a Code of Practice or other guidance to support political parties to ensure they adhere to the privacy principles around the processing of personal information.	
Journalism exemption	
17	***Does the journalism exemption appropriately balance freedom of the media to report on matters of public interest with individuals' interests in protecting their privacy?***
	No. We believe that the current exemption which relies on effective enforcement by media self-regulatory bodies is flawed. Those bodies have not adequately protected the

	rights of Australian, sometimes in the most difficult and tragic of circumstances. We believe that affected individuals should be given some direct recourse to complain and be compensated for the privacy invasive activities of media organisations (rather than relying on the inadequate and delayed response from bodies like the Press Council). We recommend that the privacy principles apply to journalists (defined to limit that application to new and investigative reporting) with an exception for public interest or benefit.
18	***Should the scope of organisations covered by the journalism exemption be altered?***
	Yes. Please refer to our answer above.
19	***Should any acts and practices of media organisations be covered by the operation of some or all of the APPs?***
	Yes. Please refer to our answer above.

Notice of Collection of Personal Information

Improving awareness of relevant matters

20	***Does notice help people to understand and manage their personal information?***
	Compliance with notified undertakings is an important area for the ACCC to use its powers to support fair conduct and protect individuals from unlawful and deceptive practices. To that extent, we support any initiatives that will help people understand what information entities are collecting and how they are using that information. However, we do not believe that notices should be relied on as part of a consent measure to manage privacy protections, to the exclusion of other protections. The efficacy of privacy notices by themselves has been much questioned (in terms of length, readability and the degree of information disclosed). Similarly, many have questioned how genuine consent can be, given the information asymmetry and power imbalance in most on-line transactions. Effective, transparent notices must be included as one of the range of privacy protective measure that should be supported by regulation, which in turn supports a level of basic protection that cannot be removed or overtaken by consent. Just as protections from unfair contract provisions apply regardless of contractual provisions to the contrary, basic privacy protections (such as collection and use limitation) should apply regardless of consumer consent.
21	***What matters should be considered to balance providing adequate information to individuals and minimising any regulatory burden?***
	The operation of APP 1 and APP5 together is somewhat unique in privacy regimes. The two principles seemingly require two separate notification obligations, one general one and one that is attached to collection. We submit that notice obligations could be simplified and improved via a detailed review of the operation of the requirements of APP 1 and APP 5.

22	***What sort of requirements should be put in place to ensure that notification is accessible; can be easily understood; and informs an individual of all relevant uses and disclosures?***
	We support the implementation of a simplified privacy notice, using clear, concise and plain-English language, at a readability level suitable for the target audience for the notice. Privacy notices should be easily understood by an individual, and should include: 1. The complete disclosure of all data being collected about an individual. This includes the disclosure of any advertising tags or cookies that can be used to identify any behavioural or interest-based attributes of the individual. 2. An easy to understand outline of the purpose for which the organisation is collecting the individual's data, including for uses that relate to advertising, website security, user experience or website performance. If the data is being collected to provide a product or service, this purpose must align to a permitted basis for processing of personal information by that organisation. 3. Information surrounding all intended uses of the individual's data. Use should be limited to the purpose that was disclosed at collection, and not for any other purpose except with the explicit consent of the user. This includes details of all parties with whom data may be shared. 4. Information about how individuals can exercise rights, including more detailed information about how to make a complaint. 5. An easy to understand outline of data retention and deletion practices. As well as simplification and readability, consideration should be given to ensuring that the right information is given at the right time. This could be done by more extensive guidance and regulatory action from the ATO. Examples of where this might apply include mobile application will involve collection of new data or a different use of data. Individuals should also be updated or reminded of the important provisions in privacy notices from time to time so they have the opportunity to ensure their use is current and that they continue to understand what their data is being collected and used for and who it is shared with.
Third party collections	
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?***
	We submit that there should be some distinction made where information being collected is already in the public domain. Where the PI collected has been made public by the individual (other than in an accidental or unintended way), then it may be appropriate that information be able to be used without requiring that the individual be notified. Additionally however, before any information that has been collected about an individual from a third party is to be used in any way that affects the individual, they should also be notified by the third party of the collection, use and other matters required in the case of a direct collection.

	There are other exceptions that should also be excluded from the notification requirement, for example, where the collection from the third party is in the context of collecting information primarily around the third party for example, providing next of kin or emergency contact information or family history as part of the provision of a health service.

Limiting information burden

24	***What measures could be used to ensure individuals receive adequate notice without being subject to information overload?***

There are many existing transparency methods which could be supported by a more active campaign by the OAIC, perhaps working with multiple agencies, to reduce issues with the length and complexity of current notices.

These include many of the techniques referred to in the issues paper such as:

- Just in time notices, and
- The use of icons and visualisations.

There are also examples of successful provision of notice of legal obligations in other industries, such as the financial services industry, which could be used to support improved privacy notices.

We would like to re-iterate again that the provision of an improved notice should not be regarded as more than meeting the requirement that organisations be transparent in regard to their processing of personal information. An improved notice and consent mechanism will never provide adequate protection for the rights and freedoms of individuals that are ensured by Australia's privacy laws. The operation of market mechanisms to enable individuals to exercise choice over the use of their personal information are not effective because the information asymmetry and power imbalance between individuals and organisations.

25	***Would a standardised framework of notice, such as standard words or icons, be effective in assisting consumers to understand how entities are using their personal information?***

Yes, we support the development of a standardised framework of notice, together with other innovative tools to support greater user control over their data. This is an area where more proactive guidance from the OAIC, leveraging insights from the customer experience space, would be of great benefit to the regulated community.

Consent to collection and use and disclosure of personal information

Consent to collection, use and disclosure of personal information

26	***Is consent an effective way for people to manage their personal information?***

Privacy 108 notes that the premise of the question may be invalid.

Privacy protection is not simply about giving people the ability to manage their personal information (as a matter of choice and consent). This is the consumer focus perspective that ignores the importance of protecting fundamental human rights as being intrinsic to the modern liberal democracy that Australia represents.

Privacy108
We Protect Privacy

Consent may be an effective way to manage consumer rights but, by itself, it is not an effective way to manage rights to privacy.

To the extent that the privacy protections recognise that consent may be relied on as one of the bases for processing, we support the strengthening of consent requirements and limiting the circumstances in which consent can be relied on.

27	***What approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed?***

We submit that the Act be amended to include a definition of consent consistent with other legislation, like that in the GDPR. In particular, consent should be defined as:

- an affirmative act of agreement
- freely given,
- specific,
- unambiguous,
- informed,
- current, and given by a person with capacity.

Approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed.

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?**

Yes, it is important that consent be 'un-bundled.'

Requiring that consent be given for each use (where there is no other legal basis for processing) is the only way of ensuring that the consent is indeed voluntary and genuine.

29	***Are the existing protections effective to stop the unnecessary collection of personal information?*** ***a. If an individual refuses to consent to their personal information being collected, used or disclosed for a purpose that is not necessary for providing the relevant product or service, should that be grounds to deny them access to that product or service?***

We submit that consent should never be the basis on which information that is not necessary for providing the relevant product or service can be collected.

Just as consent should not be necessary for the use or disclosure of personal information which is in pursuit of the primary purpose for which the information was collected in the first place, or for directly related secondary purposes, consent should not be used to support the unnecessary collection of personal information, or at least other than in very specific circumstances.

30	***What requirements should be considered to manage 'consent fatigue' of individuals?***

Limiting the circumstances in which consent must be required (e.g. where the information collected is in the public domain is) will help limit consent fatigue to the extent that it exists. The

other measures under consideration in relation to the provision of notices, such as use of icons and visualisations, and other requirements for improved readability should also prevent consent fatigue.

Again, we submit that this is an area where the OAIC could take a leading role in supporting innovative solutions to ensuring individuals understand what data is being collected and what that data will be used for. We note that the OAIC has itself said that that burden "should not fall only on individuals but must be supported by appropriate accountability obligations for entities, as well as other regulatory checks and balances".

We also submit that consent only be used in limited and exceptional circumstances. These might include where the collection:

- might be considered as unnecessarily intrusive; or
- might lead to outcomes which would be unfair or discriminatory, or which would diminish human dignity

We support the proposition that consent shifts the burden on the individual critically analyse and decide whether they should disclose their personal information in return for a service or benefit, as included in the OAIC's submission to the ACCC in response to its Customer Loyalty review.

Exceptions to the requirement to obtain consent

31	***Are the current general permitted situations and general health situations appropriate and fit-for-purpose? Should any additional situations be included?***

We believe that the current expectations to the requirement are sufficient.

Pro-consumer defaults

32	***Should entities collecting, using and disclosing personal information be required to implement pro-privacy defaults for certain uses and disclosures of personal information?***

We submit that consideration should be given to the inclusion of privacy by design and privacy by default specifically in the Australian Privacy Principles to support the implementation of pro-privacy protections in the goods and services provided by covered entities.

Obtaining consent from children

33	***Should specific requirements be introduced in relation to how entities seek consent from children?***

Children are deserving of special protection, particularly in regard to their on-line activities. Protections should go beyond seeking consent and extend, for example, to limitation of the type of information that can be collected as well as the use of information about children. In particular, consideration should be to specific regulation of tracking, monitoring, profiling or targeting of children. Children should also be given explicit and unconditional rights of erasure.

The role of consent for IoT devices and emerging technologies

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

The use of IoT devices requires significant attention from the OAIC and development of detailed guidance and support for the regulated community.

The extension of the definition of personal information to include technical information and the concept of 'identifiability' should extend the operation of the standard privacy principles to the processing of data linked to the use of IoT devices. However, as an area of significant new technical development and expanding creation and collection of data, consideration should be given to more specific regulation using principles of fairness and intrusiveness	
Inferred sensitive information	
35	**Does the Act adequately protect sensitive information? If not, what safeguards should be put in place to protect against the misuse of sensitive information?**
We believe that it may be appropriate to re-consider the definition of 'sensitive' information and whether the current protections are sufficient and appropriate.	
36	***Does the definition of 'collection' need updating to reflect that an entity could infer sensitive information?***
We submit that references to the collection of data be updated and that the term 'collection' be incorporated within the broader concept of 'processing' to remove unjustified distinctions between collection and other uses of data. This would also make the Privacy Act more consistent with other regimes, such as the GDPR.	
Direct marketing	
37	***Does the Act strike the right balance between the use of personal information in relation to direct marketing? If not, how could protections for individuals be improved?***
We submit that the regime provided by APP 7 is out of step with other privacy regulatory models and the treatment of personal information used for direct marketing under the Privacy Act should be reviewed. In particular, we submit that: • Given current concerns regarding the collection and use of data for marketing purposes, there seems little justification for APP 7 in its current form which in effect makes it easier to use personal data for marketing purposes; • The use of personal information for marketing should be subject to the same restrictions on use as apply to non-marketing information (both in terms of primary and secondary use); • There should be an explicit and unconditional right to simply and easily withdraw consent to use of personal information for marketing purposes at any time. • Consideration be given to the explicit regulation of some processing used for 'marketing' such as the more intrusive and covert tracking and profiling activities which power online behavioural advertising .	
Withdrawal of consent	
38	***Should entities be required to refresh an individual's consent on a regular basis? If so, how would this best be achieved?***
Currency is an important part of consent (whether by refreshing or other reminder about the use of PI). The same comment applies to other uses of information (even where not based on consent). If an entity continues to use personal information for an extended period after the initial collection, a reminder of that use would support transparency of processing.	

39	***Should entities be required to expressly provide individuals with the option of withdrawing consent?***

We believe that entities should be required to expressly provide individuals with the option of withdrawing consent. Express notice of the right to withdraw consent supports the voluntary nature of the decision made.

40	***Should there be some acts or practices that are prohibited regardless of consent?***

As referred to in other parts of this submission, we are strongly of the view that there are acts and practices that should be prohibited regardless of consent. These include where the processing:

- might be considered as unnecessary or excessive in the circumstances unnecessarily intrusive; or
- might lead to outcomes which would be unfair or discriminatory, or which would diminish human dignity.

Emergency declarations

41	***Is an emergency declaration appropriately framed to facilitate the sharing of information in response to an emergency or disaster and protect the privacy of individuals?***

Regulating use and disclosure

42	***Should reforms be considered to restrict uses and disclosures of personal information? If so, how should any reforms be balanced to ensure that they do not have an undue impact on the legitimate uses of personal information by entities?***

As referred to in other parts of this submission, we are strongly of the view that there are acts and practices that should be prohibited regardless of consent. These include where the processing:

- might be considered as unnecessary or excessive in the circumstances unnecessarily intrusive; or
- might lead to outcomes which would be unfair or discriminatory, or which would diminish human dignity.

Control and security of personal information

Security and retention

43	***Are the security requirements under the Act reasonable and appropriate to protect the personal information of individuals?***

The provisions in the Act are largely consistent with those in other privacy regimes.

We submit that consideration be given to differentiating between entities that make decisions around the processing of data (controllers) and those that support the processing (processors). Controllers should have some obligation to ensure contractual protections are in place with all organisations that provide processing services, including requirements as to the security of the

personal information being processed. However, both entities should have more particularised obligations in regard to how they secure the personal information they hold.

The OAIC last issued Guidance on reasonable security in July 2019. Security is a sophisticated and complex area of practice. Given the resource limitations already impacting the OAIC, it would be prudent for the responsibility for ensuing that entities properly secure their personal data, be shared with another regulatory body or government agency with more expertise in this area, such as the Australian Cyber Security Centre.

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

Please see our response above in regard to defining what is meant by 'de-identification.'

We also re-iterate that greater disclosure provisions should apply to the retention and destruction/de-identification policies of entities in regard to the personal information they hold.

Access, quality and correction

45	**Should amendments be made to the Act to enhance:** **A. transparency to individuals about what personal information is being collected and used by entities?** **B. the ability for personal information to be kept up to date or corrected?**

Right to erasure

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?***

Privacy 108 supports a general right to be forgotten subject to certain exceptions including:

- Public interest; and
- Where required for records or archiving purposes.

The inclusion of such an explicit right is consistent with similar provisions in the CDR scheme and the My Health Records Act.

Privacy 108 supports a broader right to be forgotten for children.

Privacy 108 also supports greater transparency around the times for which personal information will be retained (after which it should be destroyed or de-identified). This will provide greater transparency as to the period of retention of personal information.

47	***What considerations are necessary to achieve greater consumer control through a 'right to erasure' without negatively impacting other public interests?***

Overseas data flows and third-party certification

48	***What are the benefits and disadvantages of the current accountability approach to cross-border disclosures of personal information? Are APP 8 and section 16C still appropriately framed?***

One of the biggest issues with the current accountability approach is the lack of review or enforcement by the OAIC.

Our experience is that few Australian organisations are concerned with the operation of APP 8 and most are unaware of its application. This is in stark contrast to the operation to the cross-border data flow limitations in the GDPR and the impact they have had on entities around the world and international data flows.

49	***Is the exception to extraterritorial application of the Act in relation to acts or practices required by an applicable foreign law still appropriate?***

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

Our experience is that to date there is little understanding of or appetite for the implementation of the CPBR system in Australia. The territorial limitation of the CBPR system make it of limited interest.

51	***What would be the benefits of developing a domestic privacy certification scheme, in addition to implementing the CBPR system?***

Privacy 108 believe there is limited merit in developing a domestic privacy certification scheme. The value would only be to businesses operating within Australia, excluding those providing services to State government agencies (unless the Act is extended to apply to those services).

We support the recognition of an international independent third-party certification scheme that would allow for an accredited certification body to certify an organisation's compliance with privacy principles (such as pursuant *to ISO 27701: Privacy Information Management System*). The recognition of an independent third-party certification scheme would simplify the role of the OAIC and release valuable resources to pursue other activities. It would also give regulated entities a surer pathway to meet their compliance obligations.

We acknowledge that mechanisms such as 'privacy 'seals', 'badges' and certification have had a poor track record elsewhere, and so would proceed with caution in recognising any certification system, to ensure that it is likely to provide the benefits available from independent certification.

We also recommend that the OAIC recognise an alternative dispute resolution mechanism for individuals (as discussed above).

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

We believe that it would be in the interests of Australian organisations for this review to consider what changes might be required to achieve adequacy under the GDPR.

An adequacy finding would ease the compliance burden not only for organisations operating internationally but also for the Australian arms of multinational businesses. We believe it is worth pursuing to at least understand what changes may be required and assess the appetite of Australian businesses for such changes.

Privacy108
We Protect Privacy

Enforcement powers under the Privacy Act and role of the OAIC

53	***Is the current enforcement framework for interferences with privacy working effectively?***

The most important piece for the effective operation of a principle based regulatory system is the active engagement and support of the regulator with the regulated community.

We submit that the OAIC needs significant additional resources to enable it to support and enforce the privacy regulatory system as intended.

We also suggest that consideration be given to other methods for the conciliation of complaints. This could relieve the pressure on OAIC resources and allow it to focus on providing guidance and education and identifying and pursuing systematic issues important to the appropriate protection of privacy rights in a rapidly changing environment. Giving individuals an alternative mechanism to pursue their claim, could bring more timely and responsive action to resolve individual complaints.

54	***Does the current enforcement approach achieve the right balance between conciliating complaints, investigating systemic issues, and taking punitive action for serious non-compliance?***

It is difficult to comment on the sufficiency of the current enforcement mechanisms given their limited use to date, and the limited information available about the way they have been used.

We note that the OAIC's annual report cites improvements in the timeliness of closing complaints. However, there is little information on how the majority of privacy cases are resolved. In the past, many complaints have not been pursued, which means that statistics on the closing of complaints may not reveal the fill picture. Given there is no ability for an individual to appeal from a decision by the Commissioner to not proceed to investigate a complaint, the transparency regarding this decision making is further limited.

We also note that:

- To date there have been no investigation or reporting on systemic issues affecting the regulated community.
- Investigations that have been undertaken often involve significant delays between the collection of evidence and publication of the report (For example, the assessment of the handling of personal information as part of the PAYG Program in 2017nand 2018 will be reported on in the 2019 -2020 year – some 2 years after the fieldwork was conducted. The OAIC published a report in 2018 based on evidence of compliance collected in its 2016 review of Loyalty Programs);
- No punitive action has been taken for serious non-compliance (other than in the pending action against Facebook).

55	***Are the remedies available to the Commissioner sufficient or do the enforcement mechanisms available to the Commissioner require expansion?***

As discussed above, it is difficult to comment on the sufficiency of the current enforcement mechanisms given their limited use to date.

We support increased resourcing of the OAIC and co-operation with other regulations which might lead to more proactive use of the current enforcement mechanisms.

As discussed above we also suggest that consideration be given to an alternative method for resolution of claims, perhaps leveraging Fair Trade or Administrative Tribunals already established and resourced to support resolution of these types of claims.

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? If so, what should these expansion mechanisms look like?***

Privacy 108 supports consideration of individuals having a direct right of action under the Act. This could be by way of a combination of alternative dispute resolution mechanisms and a right to sue. The right to sue should also contemplate class actions.

Statutory tort

57	***Is a statutory tort for invasion of privacy needed?***

The necessity and terms of a statutory tort for invasion of privacy have been considered multiple times by different law reform commissions across Australia, as well as regulators.

We support the introduction of a statutory tort for invasion of privacy in terms recommended by the Australian Law Reform Commission.

58	***Should serious invasions of privacy be addressed through the criminal law or through a statutory tort?***

The right to sue should be available through a civil right rather than as part of criminal law.

59	**What types of invasions of privacy should be covered by a statutory tort?**

We support the introduction of a statutory tort for invasion of privacy in terms recommended by the Australian Law Reform Commission.

60	***Should a statutory tort of privacy apply only to intentional, reckless invasions of privacy or should it also apply to breaches of privacy as a result of negligence or gross negligence?***

We support the introduction of a statutory tort for invasion of privacy that applies to serious breaches resulting from the negligence of the entity involved.

61	***How should a statutory tort for serious invasions of privacy be balanced with competing public interests?***

We support the introduction of a statutory tort for invasion of privacy in terms recommended by the Australian Law Reform Commission.

62	***If a statutory tort for the invasion of privacy was not enacted, what other changes could be made to existing laws to provide redress for serious invasions of privacy?***

We believe that, if no statutory tort for invasion of privacy is introduced, individuals should have the right to sue for interference with privacy under the Act. The right to sue should contemplate class actions.

Notifiable Data Breaches scheme – impact and effectiveness

63	***Have entities' practices, including data security practices, changed due to the commencement of the NDB Scheme?***

Although some inferences regarding awareness of the scheme can be drawn from the number of reported data breaches, the impact of the NDB Scheme on entities practices is difficult to judge. The change in data security practices linked to the introduction of the NDB scheme would ideally be a matter that the OAIC would be able to track and report on, given that this is one of the stated objectives for the introduction.

Security is a sophisticated and complex area of practice. Given the resource limitations impacting the OAIC, it would be prudent for the responsibility for ensuing that entities properly secure their personal data and respond to data breaches as part of the NDB scheme, be shared with another regulatory body or government agency with more expertise in this area, such as the Australian Cyber Security Centre. Notwithstanding the high number of reported breaches to the OAIC, there has been no reported investigation into a data breach case since the report published in 2017 in relation to the DonateBlood.com.au data breach (Australian Red Cross Blood Service)

64	***Has the NDB Scheme raised awareness about the importance of effective data security?***

Anecdotally, the NDB Scheme has raised awareness about the importance of effective data security. However, more could be done particularly if the OAIC were able to work in collaboration with other agencies with more expertise and resources to assist in supporting cyber security practices of Australian entities.

65	***Have there been any challenges complying with the data breach notification requirements of other frameworks (including other domestic and international frameworks) in addition to the NDB Scheme?***

Lack of clarity around who has the reporting obligation where the same incident affects multiple entities has resulted in the same breach being reported multiple times to the OAIC. Development of protocols around data breach reporting to be used where, for example, a processor is affected by a NDB, would simplify the reporting procedure and reduce the impact on the OAIC.

More detailed guidance on what breaches are notifiable and the criteria for determination would also assist in determining the application of the scheme in different circumstances.

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 plays an important independent role as the primary regulation addressing privacy protection in Australia. That role should be maintained.

67	***Is there a need for greater harmonisation of privacy protections under Commonwealth law? If so, is this need specific to certain types of personal information?***

It would be of great assistance to the regulated community if State and Commonwealth privacy laws were harmonised.

Not only are the differences between the different regimes difficult for Australian businesses to navigate, there are also large gaps left by operation of the current laws including: • State government entities in WA and SA not being subject to any legal requirement in regard to the protection of the personal information they hold; and • The exclusion of contracted service providers to State government agencies from the Commonwealth Act regardless of whether or not those CSP's have accepted obligations pursuant to State regimes (where they exist).	
69	***Are the compliance obligations in certain sectors proportionate and appropriate to public expectations?***