Australian Privacy Foundation

Bringing Australia's *Privacy Act* up to international standards

(Submission in response to the *Privacy Act Review - Issues Paper*)

Graham Greenleaf, Nigel Waters, Kat Lane, Bruce Arnold, and Roger Clarke

18 December 2020

Bringing Australia's *Privacy Act* up to international standards (Submission in response to the *Privacy Act Review - Issues Paper*)

Australian Privacy Foundation

17 December 2020

1. About the Australian Privacy Foundation and this submission

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. Information about the APF appears at the end of this submission.

This submission to the Government is by the APF in response to the Attorney-General's *Review of the Privacy Act 1988 (Cth) – Issues Paper*.[1] The authors, with expertise in privacy-related regulation and trust issues, who have contributed to this submission are: Graham Greenleaf, Nigel Waters, Kat Lane, Bruce Arnold, and Roger Clarke. The APF has made previous submissions on these issues to the ACCC and the government,[2] in response to the ACCC *Digital Platforms Inquiry* and the ACCC *Customer Loyalty Schemes Review,*[3] and they inform this submission. It is consistent with a range of detailed official and civil society analyses over the past few years, as detailed in those previous submissions.

The APF gives general support and endorsement to the submissions in response to this review by Salinger Privacy (Anna Johnston)[4] by Dr Katherine Kemp[5], and by A/Prof Mark Burdon and Tegan Cohen.[6]

APF also agrees with and supports many recommendations made by the Office of the Australian Information Commissioner (OAIC) [7] but we disagree with other OAIC recommendations. We have noted in this submission particular aspect to which we give support, and others we oppose. The OAIC submission has only been available for a week, and is complex (70 recommendations), so APF may on further consideration alter its view of some of these when it makes a submission on the Discussion Paper in 2021.

2. General observations

2.1. The need for a comprehensive review of the Privacy Act

The last comprehensive review of the Privacy Act was in 2008 with the publication of the Australian Law Reform Commission Report *for Your Information – Australian Privacy Law and Practice*[8] (the ALRC Report). The ALRC report recognised privacy as a human right. It also found that privacy protection should take precedence over a range of countervailing interests,

---

[1] Attorney-General (Australia) *Review of the Privacy Act 1988 (Cth) – Issues Paper,* 30 October 2020 <https://www.ag.gov.au/integrity/publications/review-privacy-act-1988-cth-issues-paper?mc_cid=8701356c4f&mc_eid=cf48d8dbfa>

[2] APF 'Regulation of digital platforms as part of economy-wide reforms to Australia's failed privacy laws Australian Privacy Foundation submission to the Australian Government on implementation of the ACCC's *Digital Platforms Inquiry—Final Report*' 10 September 2019 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3341044> ; 'Australian Privacy Foundation submission on ACCC draft report 'Digital Platforms: The Need to Restrict Surveillance Capitalism', 22 February 2019 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3341044> .

[3] ACCC Digital Platforms Inquiry <https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry>; ACCC Customer loyalty schemes review https://www.accc.gov.au/focus-areas/market-studies/customer-loyalty-schemes-review.

[4] Salinger Privacy *Submission in Response to the Privacy Act Review – Issues Paper, October 2020* <https://www.salingerprivacy.com.au/wp-content/uploads/2020/11/20-11-20_Privacy-Act-review_Salinger-Privacy_Submission.pdf>

[5] Katharine Kemp *Making the Australian Privacy Act fit for the digital era*' 7 December 2020

[6] Mark Burdon and Tegan Cohen *Issues Paper Submission - Attorney General's Department - Review Of The Privacy Act 1988 (Cth),* QUT School of Law/Digital Media Research Centre

[7] Angelene Falk, Australian Information Commissioner and Privacy Commissioner *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner* 11 December 2020

[8] Available at https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/.

such as cost and convenience. However, although the government at the time professed to accept many of the ALRC's recommendations, and said it would introduce legislation in a number of tranches, it failed to introduce many of the most important reforms, such as removal of exemptions. APF submits that, after this Review, the government should introduce one comprehensive reform Bill, and should not resort to the subterfuge of reform in stages.

Significantly, since 2008, many countries have introduced stronger privacy protections for their people. For example, the European Union (EU) has introduced significant privacy protections in the General Data Protection Regulation (GDPR). These laws are regarded as the gold standard in best practice data protection. The GDPR commenced operation in 2016 and was fully implemented across the EU by 2018.

In comparison, Australia's privacy and data protection laws are weak and do not meet the best practice standards set by the EU and other countries. This review must be used as an opportunity to modernize and strengthen Australia's privacy laws to meet the best practice standards set Internationally. Australia should even seek to exceed those standards and lead the world.

We would also add that there are considerable advantages for Australia in at least aligning our privacy protection to the GDPR including:

- A clear signal to Australia's trading partners that we take data protection seriously.
- The negotiation of a free trade agreement would mean we have the same standards.
- Other countries who have already made similar agreements with the EU would have certainty on the standards being applied.
- It would reduce the complications faced by businesses in Australia who operate internationally, in relation to data exports, and to alignment between standards applied by their Australian and overseas offices.

2.2. Australian Charter of Human Rights

Privacy is a human right. The right to privacy is articulated in several international human rights instruments[9]. However, in Australia we do not have national human rights legislation, any embedded human rights in our Constitution, or State/Territory legislation that is strong enough. The APF supports the campaign for an Australian Charter of Human Rights. Human rights legislation is needed so Australians (like citizens of other countries like the United Kingdom[10] and the United States of America[11]) can ensure that all legislation is tested against human rights[12].

2.3. Terms of Reference

The terms of reference do consider some major issues but it excludes other critical privacy related problems including:

1. Best practice approaches internationally

[9] Some examples: Article 12 of the United Nations Declaration of Human Rights 1948 Article 12, International Covenant of Civil and Political Rights 1966 Article 17; United Nations Convention on Migrant Workers Article 14; United Nations Convention on the Rights of the Child Article 16.

[10] Human Rights Act 1998 (UK) at https://www.legislation.gov.uk/ukpga/1998/42/contents.

[11] United States of America: The Constitution at https://www.whitehouse.gov/about-the-white-house/the-constitution/.

[12] It is of significant concern that Australia has been able to enact legislation that could not be enacted in other countries with constitutional or legislative human rights protections. For example, the following legislation could not be enacted (or would be successfully challenged) in the UK or the USA like the Assistance and Access Act 2018 and the Telecommunications (interception and Access) Act 1979.

2. Privacy protections in the COVID-19 pandemic (the pandemic)
3. The COVIDSafe app

The terms of reference should not have excluded the above matters. It is essential that even qualified human rights are preserved in a pandemic. We have covered those issues in our submission at "Other issues" and we urge the Attorney-General's Department to consider our submissions. The exclusion of the COVIDSafe app is particularly perplexing (and ironic) given that a very healthy debate about privacy when it was introduced actually led to a particularly rigorous privacy regime and safeguards which can be seen as a useful model.

2.4. Funding for the Office of the Australian Information Commissioner (OAIC)

As can be seen from the name of the regulator, privacy is only a secondary consideration. By world and Australian standards, the OAIC is a weak regulator. Some of this is no doubt due to a lack of adequate funding and the numerous attempts to move and diminish the role of the dedicated Privacy Commissioner. Regrettably, more than 20 years of 'brand awareness' of privacy in the community was sacrificed when the role was subsumed under the OAIC.

The OAIC needs to have adequate funding, strong powers, a regulator culture similar to the ACCC and, high compensation limits. The OAIC needs to be a strong regulator, and the review of the Privacy Act must be followed with adequate funding of the OAIC.

APF submits that the title of the office should refer to 'Information and Privacy Commissioner' rather than just 'Information Commissioner', and that the review of the Privacy Act should be followed by adequate funding of the office.

2.5. The ACCC Digital Platform Inquiry

The APF gives strong support to the importance of the problems identified by the ACCC in the Digital Platform Inquiry. The privacy implications of the role of digital platforms is well-analysed by Dr Katherine Kemp, in her submission (section 1), and APF endorses her analysis.

In the final report the ACCC concluded that both Google and Facebook have substantial market power. We submit that it is essential that the Government give full weight to all of the companies that these two businesses have acquired, and also to all the streams of personal information to which they have access because of those acquisitions and because of other business arrangements.

With the emergence of the data economy, the collection and use of personal data represent the main source of value for digital platforms. The effective control of large data sets exercised by platforms, such as Google and Facebook, supports and reinforces network effects and the substantial market power possessed by platforms. Moreover, the market power of the platforms creates a power imbalance between platforms and users such that any consent given by users to the collection and use of personal data is illusory. Establishing an effective data privacy regime is therefore essential to correct market imperfections in the data economy.

The APF considers, however, that the issues at stake also go beyond questions of correcting market imperfections, and that the government should explicitly recognise that they constitute a new and dangerous economic formation. These flows of data have been used to create what is now widely described as 'the surveillance economy' (or 'surveillance capitalism'[13]) substantially invented by Google nearly two decades ago, and shortly thereafter

[13] The mechanisms of surveillance capitalism are explained in the most comprehensive detail by Shoshana Zuboff *The Age of Surveillance Capitalism* (Public Affairs, NY, 2019), and in her earlier articles. Zuboff argues that surveillance capitalism is a new form of capitalism distinguished by its extraction and exploitation of 'behavioural surplus' (personal data collected for

adopted by Facebook, which are still its dominant exponents. They are the most significant providers of both data and data acquisition channels to the market for surveillance services, as distinct from their imitators, and the many purchasers of those services, who also contribute to the resulting problems. In relevant recent developments, German regulators have ordered Facebook to restrict data collection, by requiring that express user consent be obtained before combining WhatsApp, Instagram, and Facebook account data.[14]

There are three aspects of the surveillance economy that are of particular relevance to the reforms it is necessary for the Government to now implement:

(i) its mechanisms compel the providers to a market for surveillance services to constantly seek to expand the scope of their collection of behavioural data, thus creating market power risks;

(ii) the nature and sources of data used by those with access to surveillance market data (particularly Facebook and Google) are largely invisible to those consumers and citizens involved in transactions with them, thus exacerbating privacy risks and problems of effective privacy regulation; and

(iii) the global operation of leading digital platforms, which provide these corporations with both sufficient revenue to disregard small scale penalties, and a strong incentive to engage in regulatory arbitrage, in particular to resist effective regulation in a jurisdiction such as Australia because an effective regime here is likely to influence policymakers in existing or emerging markets.

More broadly, failure by Government to effectively address these issues will serve to erode the trust that is fundamental to electronic commerce, and to the engagement by citizens with e-government initiatives. Erosion of trust in digital platforms arising from insufficient protection of personal information is not simply confined to chilling e-commerce, but extends to broader trust deficits in digital services, such as digital health services and electronic services, and more generally to undermining trust in Government.

The APF submits that the Government should be conscious of the global and regional dimensions of these issues, which present both challenges and opportunities for effective regulation (e.g. consistency with practice in the European Union and recognition that corporations such as Facebook have consistently demonstrated a willingness to evade responsibility by claiming that they operate outside EU law). Furthermore, in developing an effective regulatory regime the Government should be conscious that digital platforms are susceptible to misuse for 'fake news' (including inappropriate political communication and data gathering, whether directly by the platform operator or by that operator's partners), and that privacy involves more than concerns about undisclosed or deceptive data gathering for direct marketing.

2.6. The ACCC Customer Loyalty Schemes Review

The Final Report of the review of Customer loyalty schemes was released in December 2019.[15] The report found that loyalty schemes were "collecting, using and disclosing data in

---

the primary purpose of predicting and changing individual behaviours, rather than for the primary purpose of improving a service to individual users). She argues that one of the principal dangers of surveillance capitalism is that its key practitioners are compelled to expand the extent of their surveillance of individuals in order to maintain their dominant positions.

[14] Alex Hern 'German regulator orders Facebook to restrict data collection' *The Guardian*, 7 February 2019 <https://www.theguardian.com/technology/2019/feb/07/german-regulator-orders-facebook-to-restrict-data-collection>

[15] Available at https://www.accc.gov.au/system/files/Customer%20Loyalty%20Schemes%20-%20Final%20Report%20-%20December%202019.PDF.

ways that do not align with consumers' preferences".[16] This is in effect a systemic breach of the privacy of the millions of people who use these schemes. Recommendations 3 to 5 all concerned improvements in privacy protections.

3. Responses to list of questions

3.1. 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?

The current objects of the Privacy Act are unnecessarily narrow in scope and weak. The objects need to be redrafted to reflect a strong commitment to privacy and data protection. APF endorses OAIC recommendations 1-3 for reform of these objects.

APF further recommends the following changes to the objects to better reflect modern issues with privacy and data protection.

- The objects recognise privacy and data protection as a human right. Australia recognises its human rights obligations through various international instruments. The GDPR recognises "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."[17]
- Data protection should be a specific object
- We support the ACCC's call for an objective to be to empower people to make informed choices.
- It is not clear what object 2A(a) actually means and whether it has ever happened.
- We support the ACCC's call for the object 2A(b) to be revised as it is inappropriate for privacy and data protection to be "balanced" with the interests of business. Privacy and data protection are human rights whereas running a business is a commercial enterprise. Human rights must prevail over business needs.
- Object 2A(f) is manifestly inadequate. "Respect" for privacy should not be an object. Strong wording is needed.
- Object 2A(g) needs significant revision to require the right to complain, and that complaint will be decided and complainants compensated for any loss.

3.2. 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 a critical issue. If the information does not meet the definition of personal information, then the protections in the Privacy Act do not apply. If there is a narrow definition or interpretation of the definition of personal information it necessarily follows that the Privacy Act will fail to protect people from a range of privacy issues. For these reasons, the definition of personal information must be as wide as possible.

[16] Page iv of the ACCC Customer loyal schemes – Final report

[17] Article 1 of the GDPR at https://gdpr-info.eu/

The APF supports the replacement of the current definition of 'personal information' with either of two alternatives: (i) the definition used in the GDPR; or (ii) the definition proposed by Salinger Privacy.

(i) The APF supports the use of a similar definition as that used in the GDPR for personal data:

> *Personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by references to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

It would be the preference of the APF to completely redraft the definition of personal information and change it to the personal data definition used by the GDPR. One major advantage is that it would then be more likely that the interpretation of the definition would remain consistent with the interpretation of the GDPR definition, reducing the likelihood of Australian law becoming out of step with international standards.

The current definition of personal information has already been shown in litigation (*Telstra v Privacy Commissioner*[18]) to be not fit for purpose. The narrow reading of the wording of the definition meant that "subject matter" was unnecessarily narrowed to exclude metadata. This type of problem must be avoided in future by using a broad definition.

(ii) Alternatively, APF also supports the revised definition in the Salinger Privacy submission (p. 5):

> *"personal information" means information or an opinion which relates to an identified or identifiable individual:*
> *(a) whether the information or opinion is true or not; and*
> *(b) whether the information or opinion is recorded in a material form or not; and*
> *(c) whether the information or opinion is provided, collected, created, generated or inferred.*

As Salinger Privacy argues 'Removing the concept of 'reasonably' identifiable brings the definition into line with the GDPR and multiple other jurisdictions.'

Sub-clause (c) of this definition is what is endorsed by OAIC Recommendations 6 and 7. APF submits that, if the GDPR definition is preferred, this sub-clause should be added to it.

In summary, we recommend a wide definition of personal information that is aligned to the approach of the GDPR. Any accompanying regulatory statement must make it clear that the definition is intended to be wide in scope and cover all associated technical information including technical data, inferred and generated data, and online identifiers.

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

As stated above, we support the definition being wide and covering inferred personal information. Specific inclusion of inferred personal information has important implications for the operation of the collection APPs, as inferred information is arguably not 'collected' – see below. As Salinger Privacy argues: "This amendment would make explicit that inferences drawn from data, or new data generated about an individual (such as customer insights which lead to ratings being applied to a customer profile), are within the scope of the definition.'

[18] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 ('Grubb Case')

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

APF submits that, at a minimum, Australia's anonymisation provisions should be aligned with those of the European Union's GDPR. The GDPR makes a clear distinction between (i) anonymous information (Recital 26), which is not personal information; and (ii) pseudonymised information or de-identified (but re-identifiable) jnformation, both of which are personal information.

However, APF submits that there is a clear need for additional protections.. We observe that:

1. Recognising and accepting that there is now enormous evidence that de-identified data can often be re-identified and is increasingly likely to be able to be re-identified as time passes.

There have been two recent high-profile cases where de-identified data has been re-identified in Australia. There were the MyKi[19] and MBS/PBS data[20] re-identifications. This follows similar problems internationally where data is repeatedly re-identified. It is so common and so extensively written about there have been systematic literature reviews.[21]

For this reason, the term de-identified now has no place in modern privacy approaches. It is inevitable that de-identified data will be re-identified. Everyone needs to change their approach to making data anonymised and make it impossible for it to ever be re-identified.

APF submits that de-identification be removed as a definition in the Privacy Act to send a clear signal to everyone dealing with data that it must be anonymised. OAIC recommendation 8 is the same.

However, given the constantly changing technical difficulties in ensuring that anonymisation is in fact effective, APF endorses the OAIC's recommendations 9 and 10 that (i) APP 1 should require notice to individuals 'that their information may be anonymised and used for purposes other than those permitted for the initial collection' – but only where such anonymisation is intended to occur; and (ii) APP 11 should include obligations to provide reasonable security protections for any personal information that has in fact been anonymised. A form of such security requirements have been added to the laws of Japan and South Korea. APF adds that failure to do so should be an interference with privacy of the persons whose data has been anonymised.

2. Prevention is the best way to avoid re-identification. This means deleting data that is no longer needed and avoiding using sensitive data.

Deletion and erasure are covered later in this submission. However, the best way to avoid data breaches and re-identification is to ensure that people have the right to delete data.

3. Changing the definitions to remove references to 'de-identified', and instead using 'anonymous' which means no individual can be identified from the data.

This is discussed above.

---

[19] See report by the Office of the Victorian Information Commissioner 15 August 2019 at https://ovic.vic.gov.au/wp-content/uploads/2019/08/Report-of-investigation_disclosure-of-myki-travel-information.pdf.

[20] See article at https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records.

[21] For example *Re-identification attacks – A systematic literature review* at https://www.sciencedirect.com/science/article/abs/pii/S0268401215301262

4. Giving individuals a clear right to compensation and other remedial actions if purportedly anonymised data is ever re-identified.

This is addressed in part under (1) above, but two further protections are required, as recommended by OAIC:

(i) Prohibition on re-identification of anonymised data, except 'in order to conduct testing of the effectiveness of security safeguards' (OAIC recommendation 11). Security researchers must not be punished for exposing faulty anonymisation.
(ii) Adding failures of anonymisation to compulsory data breach notification requirements (OAIC recommendation 12).

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

APF submits that the definition of 'personal information' in the *Privacy Act* ought to be amended to clarify that it encompasses data drawn from the profiling or tracking of behaviours or movements such that an individual can be singled out (i.e. disambiguated from a crowd or cohort) and thus can be subjected to targeting or intervention, even if an individual cannot be 'identified', in the conventional sense, from the data or related data. The Government should consider such an amendment, which would place Australia's Privacy Act on a par with the best laws dealing effectively with the harms which the ACCC has identified.

It should be sufficient for the definition of 'personal information' that an entity is able take customised action, such as delivering a message to an individual, or responding to or interacting with an individual in other ways, where that interaction is based on knowledge of their unique identity and attributes. The potential harm (or benefit) to an individual from use of personal information does not depend on the user specifically knowing (or being able to establish) their actual identity. The key factor is that the information particular to that individual is used to enable interaction with them as individuals (whether identifiable or not).[22]

In Salinger Privacy's submission (pp. 5-6, and articles cited therein), this approach is described as adding 'individuation' to the underlying concept of 'identifiability' in the definition of 'personal information'. Whether this expansion to the concept it is best described as enabling 'individuation' or as enabling 'interaction on an individual basis' is arguable, but either would be a considerable improvement.

APF endorses the proposals made by Salinger Privacy that a definition of the word 'identifiable' should be included in the Act (so as to be read with the definition of 'personal information', as follows (modified by APF by addition of the words 'or interacted with' in italics):

> "(i) able to be identified, or (ii) able to be discerned or recognised *or interacted with* as an individual distinct from others, regardless of whether their identity can be ascertained or verified"

[22] For an example of where this concept has been used to go beyond 'identifiability', see "Personal information' – A conventional or 'revolutionary' definition?' in G. Greenleaf, and S. Livingston, 'China's Personal Information Standard: The Long March to a Privacy Law' (2017) 150 *Privacy Laws & Business International Report* 25-28, <https://ssrn.com/abstract=3128593>

APF rejects OAIC recommendation 13 that 'personal information' should include that of deceased persons. This is (almost) completely out of step with data privacy laws the world over, including the GDPR, and should not be done by a side-wind in the course of this review.

3.3. Flexibility of the APPs in regulating and protecting privacy

The OAIC in its submission makes various recommendations (14-25) concerning the APPs, most of which are not covered by the Questions asked in the Issues Paper. APF submits that the issues raised by the OAIC should be considered in the Discussion Paper.

APF endorses the following recommendations by the OAIC, subject to appropriate drafting:

- #14 – More flexibility for OAIC's involvement in Code development;
- #16 – Requiring entities to consider Guidelines issued by Commissioner;
- #17 – Greater responsibility on entities to ensure that personal data collected by others was collected in accordance with the Act;
- #19 – Absolute right of individuals to object to direct marketing uses;
- #23 – Introduction of a right of erasure. APF submits that this right should, as in the GDPR, include what is generally known as the 'right to be forgotten', which is now established as part of the laws of many countries;
- #24 – Notification of the right to erasure;
- #25 – Introduction of a right to object (Note this overlaps with recommendation 19); APF submits that consistency with the GDPR right to object is desirable;
- #26 – Notification of this right to object.

Other OAIC recommendations to give the Commissioner powers to make binding rules (recommendations 15, 18, 20, 21) should be considered, but APF submits that there must be a mechanism for such rules to be challenged by any parties that wish to do so, and for a court or tribunal to decide whether the rules are reasonable and consistent with the Act.

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?***

APF's overall position is that the Act and the Australian Privacy Principles (APPs) have not been effective in delivering strong privacy protection for people in Australia. It is likely that the problem is a combination of a weak and underfunded regulator combined with overly general principles that are interpreted narrowly, plus wide and unnecessary exemptions. Over-reliance on a 'notice and consent' model has also contributed to the Act's failure.

APF submits that there are significant gaps in the Act's coverage, which should be remedied, in relation to when private sector organisations are operating as a contracted service provider under a State or Territory contract. As Salinger Privacy identifies (p. 9), 'the practices involved in fulfilling that State contract are exempt from the Privacy Act (s. 7B(5)). However this does not necessarily mean that they are bound by a State law equivalent to the Privacy Act. They may be entirely *un*regulated for those practices.' This exemption, which Salinger Privacy documents with a variety of examples, leads to a wide range of inconsistencies in whether *any* privacy law applies in many situations where privacy protections clearly should apply. This Review is the ideal opportunity to ensure that privacy protections are comprehensive. The 's. 7B(5) exemption' should join the list of exemptions discussed below that is amended or deleted, with the aim of ensuring comprehensive coverage of privacy laws.

APF submits that the Review should also consider and deal with other areas of uncertainty and inconsistency between federal and State powers in relation to privacy issues, which do not stem from private sector contracts with State bodies. For example, most State and Territory governments are currently requiring all restaurants and other venues (private sector bodies) to utilise QR Codes for COVID-19 check in requirements, but failing to require privacy protections which are in any way comparable with the COVIDSafe Act (Part VIIIA Privacy Act) protections in relation to the COVIDSafe app.

3.4. Exemptions

Removal of the many unjustifiable exemptions from the Privacy Act was one of the major recommendations of the Australian Law Reform Commission in its review of the Privacy Act over a decade ago. This is an overdue reform. We note (and endorse) that the OAIC has recommended complete removal of the small business, employee records, and political parties exemptions (Recommendations 27-29). These exemption present an impossible hurdle, if Australia wants the international compatibility/interoperability provided by an EU 'adequacy' finding.

APF also supports the continuation of ability to apply provisions protecting privacy to exempt entities or practices both through Regulations and through APP Codes.

APF submits that all the current exemptions discussed below should be removed at least in part (and in many cases, completely): there should be no 'privacy-free zones' when personal information is used without any constraints or safeguards. In almost all cases APF argues for a complete revocation of an exemption. APPs such as security obligation should clearly apply in all cases, with compliance to be tested against the 'reasonableness' qualifier in the APP.

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?***

The so-called 'small business exemption' is a major impediment to Australia obtaining a positive adequacy assessment from the EU. Provisions in Japan's laws with similar effect were removed from its law prior to its adequacy application. No other countries have equivalent exemptions in their data privacy laws.

The other large problem is the assumption that "small business" are not large-scale data users and sellers. Business with turnovers of less than $3M can now be involved in processing vast quantities of personal information The exemptions must be removed. Consideration could be given to providing small businesses with assistance to comply (see below)

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?***

APF submits that the exemption should not be amended to use other thresholds, but should simply be abolished.

9. ***Are there businesses or acts and practices that should or should not be covered by the small business exemption?***

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?***

APF supports a removal of the exemption for small business generally, rather than exempting small businesses from only some of the APPs.

APF endorses the alternative approach suggested by Salinger Privacy (p. 11) that 'the OAIC should be significantly better funded to help proactively assist small businesses understand their obligations, as well as to respond to any increase in privacy complaints.'

11. ***Would there be benefits to small business if they were required to comply with some or all of the APPs?***

Many small businesses involved with clients outside Australia would benefit if the abolition of the exemption helped lead to an 'adequacy' decision for Australia from the European Commission, and from any equivalent decisions allowing data exports based on the country of the recipient (as is now the case in many of the 144 countries currently with data privacy laws). Cross-border data flows, either from the EU or from these other countries, would then become straight-forward by comparison with the case-by-case contractual arrangements now required.

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?***

It is critical that small businesses that trade in personal information must be required to fully comply with the Privacy Act. The ACCC has comprehensively identified that obtaining consent, for example the customer loyalty programs, does not mean they have obtained meaningful or informed consent. APF submits that consumers should not be asked to surrender their rights, and firmly opposes the use of spurious 'consent' exceptions.

Employee records exemption

13. ***Is the personal information of employees adequately protected by the current scope of the employee records exemption?***

14. ***If enhanced protections are required, how should concerns about employees' ability to freely consent to employers' collection of their personal information be addressed?***

15. ***Should some but not all of the APPs apply to employee records, or certain types of employee records?***

The scope of 'employment information' is now vast compared to what it was in 2001 when the Act first applied to the private sector, and 'employment information' now has a strong overlap with social media information, and other information gathered by intrusive surveillance. Also, some aspects of employment records already come within the Privacy Act, in relation to areas such as Tax File Numbers, and mandatory notifiable data breaches. As with the so-called 'small business' exemption, the exemption for employment records diminishes Australia's prospects of obtaining a positive 'adequacy' decisions from the EU, and similar decisions by other countries from which Australia wishes to obtain simplified cross-border data flows.

For all of these reasons, this exemption is harmful, and APF submits it should be repealed. Some aspects of employment could be included as a legitimate ground of processing (which is preferable to spurious 'consent'), and would mean that most aspects of the APPs would continue to apply.

Political parties' exemption

16. Should political acts and practices continue to be exempted from the operation of some or all of the APPs?

APF submits that it is essential that the exemption for political parties is abolished. Since 2001 the potential for personal information to be manipulated so as to influence the behaviour of voters in non-transparent ways, and potentially damage democratic political processes, has increased exponentially, as exemplified in the Cambridge Analytica/Facebook scandal.

It is very difficult to see any convincing arguments against the application of such aspects of the APPs as transparency in collection practices, observance of limits on use of sensitive data, and provision of data security.

We highlight the hypocrisy of this exemption: if provision of privacy protection is necessary for everyone else, then why not politicians and political parties? APF supports the previous ALRC recommendation for removal of the exemption, noting the caveat concerning the implied freedom of political communication, and that it will be largely irrelevant in relation to application of the APPs.

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?

18. Should the scope of organisations covered by the journalism exemption be altered?

19. Should any acts and practices of media organisations be covered by the operation of some or all of the APPs?

The condition embodied in the exemption in s.7B(4)(b), requiring merely that 'the organisation is publicly committed to observe standards', is farcically inadequate, and APF submits it should be repealed. However, there must be properly customised legal authorisation for specific practices in order to protect the public interest in reporting, and to respect the protection of political communications. Hong Kong's Ordinance provides some good examples. The OAIC recommends 'greater enforceability' against media organisations (Recommendation 30).

Based on APF's experience, it has previously concluded[23] that:

- detailed guidance is necessary
- a Framework and Guidelines need to be applied to all media
- a comprehensive, graduated range of sanctions is necessary
- complaints schemes must be credibly independent of the organisations and individuals that are subject to the regulation, and complaint determinations must be appealable

[23] APF's policy statement on Privacy and the Media https://privacy.org.au/policies/media/

- the APC does not provide adequate guidance, and any that may exist in the broadcasting field is seriously inadequate
- the existing self-regulatory and co-regulatory schemes (i.e. that operated by the APC, and the broadcasting codes administered by ACMA under s. 123 of the Broadcasting Services Act) have not satisfied these requirements

APF submits that the recommendations made by Salinger Privacy (p. 13) will remedy these problems in part:

(i) 'that the journalism exemption should be abolished, and replaced with a limited exemption to the collection, use and disclosure principles (APPs 3, 5 and 6) for activities necessary to the conduct of investigative and public interest journalism'. (APF notes that Hong Kong's Ordinance has useful provisions on this.)

(ii) 'that existing member-based media industry complaints-handling bodies such as the Australian Press Council could be recognised under s.35A of the Privacy Act as offering an external dispute resolution scheme for investigating and conciliating complaints about breaches of the APPs, so long as effective appeal rights are also established so that complainants can seek enforceable remedies'. (The OAIC Recommendation 30 also suggests this.)

3.5. Notice of Collection of Personal Information

While APF supports better transparency in relation to processing of personal information, we submit and stress that 'notice and consent' alone is not a sufficient basis for a modern data privacy law. The complementary actions needed are dealt with in more detail under 3.6.

Improving awareness of relevant matters

As Salinger Privacy put it in their submission (p. 14): "While transparency is important, we submit that this review should not overestimate the effectiveness of notice as a mechanism for delivering meaningful privacy protective outcomes for individuals."

It is necessary for two parallel steps to be taken: to significantly strengthen notice and consent, and to complement it with a variant on the GDPR's defined heads of 'legitimate processing'.

20. Does notice help people to understand and manage their personal information?

21. What matters should be considered to balance providing adequate information to individuals and minimising any regulatory burden?

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?

APF submits that legislation should specify that notice is given of the identity and contact details of the entity collecting data; the types of data collected and the purposes for which each type of data is collected, and whether the data will be disclosed to any third parties and, if so, which third parties and for what purposes. It is essential that individuals be told the purposes for which their personal data is collected, so that they can insist that the collector should only use the data for that purpose (subject to legislative exceptions). Such informed consent and consequent control reaffirms individual autonomy and serves to build trust in online interactions across the public and private sectors, a trust weakened by public awareness of recurrent large-scale data breaches and other problems involving large organisations.

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?*

If there is third party collection there should also be a duty on the APP entity to require (by contract or otherwise) the third party to deliver the notice. A third-party collector may not itself be an APP entity, so the obligation needs to rest with the APP entity.

Limiting information burden

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

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?***

The Salinger Privacy submission (pp. 15-17) includes a valuable discussion of the use of icons etc in privacy notices, including the automation of use of consumer privacy preferences. APF is generally supportive of further exploration of standardized icons which are legally binding, similar to the approach of Creative Commons icons.

However, APF submits such indicators of consumer preferences should not be used to automatically 'consent' to disclose personal data to websites etc when they are visited. This approach is very similar to the Platform for Privacy Preferences (PPP) of the late 1990s, which was not successful. Consent should be explicit and dependent on context, not a matter of automated inferences.

3.6. Consent to collection and use and disclosure of personal information

The GDPR (and many other new laws influenced by it) laces heavy emphasis on a set of defined heads of 'legitimate processing', of which 'consent' is only one head, and the others are 'non-consensual' legitimate processing (GDPR art. 6). Consent alone is rarely sufficient in relation to processing of sensitive information (GDPR art. 9). This is accompanied by a more strict definition of 'consent' (GDPR art. 7),

The Issues Paper does not contemplate such an approach. APF submits that this review of the Privacy Act should take the approach of the GDPR, and exercise tight control over the heads of legitimate processing.

The OAIC's submission proposes that consent should play a more limited role than at present, when it say 'reliance on consent should be targeted and limited to situations where individuals can and should validly exercise a choice, not expanded and used more broadly to permit data handling practices' (Executive Summary). It recommends limiting 'the use of consent for high privacy risk situations, rather than routine personal information handling' (Recommendation 31). Such an approach, if misused, can be very dangerous if it results in a profusion of types of non-consensual justifications for processing.

However, OAIC does not then propose to introduce heads of legitimate processing. Instead, it proposes an indirect approach which might achieve something similar:

(i) Considerably stronger requirements for 'consent' (recommendation 34) and for notice (recommendations 31—33), and related major improvement such as obligatory default settings (recommendation 35) and strong rights to withdraw consent (recommendation 36).

(ii) Positive requirements that all collection, use and disclosure of personal information must be 'fair and reasonable', *even if it is with consent* (recommendation 37), with the Act including a list of factors the Commissioner (or a court, APF assumes) must consider in assessing what is 'fair and reasonable' (recommendation 38), and an obligation on APP entities to implement corresponding practices (APF notes this is part of 'demonstrable accountability in EU terms) (recommendation 38).

(iii) Prohibitions on practices (five types are listed), which in effect are deemed to be not 'fair and reasonable', and which can also be seen to make them 'illegitimate grounds of processing' (Recommendation 40).

In APF's interpretation, this combination of positive requirements of 'fair and reasonable' processing (irrespective of consent, which is also more strictly defined), and negative prohibitions of processing deemed to be not 'fair and reasonable' (and for which consent is irrelevant), could approximate the GDPR's 'heads of legitimate processing', but only if the ideas were fully articulated, and all elements were expressed in law.

APF considers that the OAIC proposals require further restrictions to avoid abuses:

(a) 'Fair and reasonable' requires statutory definition of each of the necessary elements, not just a list of factors the Commissioner or Court must take into account.

(b) The enormous range exceptions for processing 'authorised or required by other laws' by the Privacy Act should also be made subject to this statutorily defined 'fair and reasonable' test.

(c) All future legislative exceptions should be made subject to a requirement that they explicitly state that they are exceptions to the Privacy Act, and also be subject to the operation of the 'fair and reasonable' test (unless they explicitly exclude it). Section 94ZD *Privacy Act*, inserted by the *COVIDSafe Act*, is a model for such a provision.

APF could support this Review taking either of two alternative approaches to reducing sole reliance on 'notice and consent', subject of course to appropriate drafting: (i) the GDPR approach of 'heads of legitimate processing'; or (ii) the OAIC's 'fair and reasonable' processing approach (Recommendations 31-40), subject to the caveats expressed above. The APF submits that the Discussion Paper should consider whether one or the other approach (or an amalgam) should be adopted. It should ensure that 'notice and consent' and 'other laws' need to be complemented by further such controls over the justification of processing under the Privacy Act.

If any such reform occurs, it is essential that it be accompanied by the 'direct right of action' reform (see 3.10). It is essential that data subjects be able to go directly to the courts to obtain interpretation of 'fair and reasonable' in particular context, and not to be forced to accept the Commissioner's interpretation.

Consent to collection, use and disclosure of personal information

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

27. What 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?

APF notes the discussion of deficiencies in the current 'notice and consent' approach, and the many valuable examples, included by Dr Katherine Kemp in her submission (Section 3).

Firstly, there are many circumstances in which organisations are permitted to perform acts that are privacy-invasive, without adequate controls and safeguards in place. Our comments in the previous section address those issues.

Further, a great deal of research shows that the notion of consent has been permitted to be debased, resulting in the 'notice and consent' approach frequently being rendered ineffective. It is essential that action be taken to overcome these issues. The key issues to be addressed are:

(i) consent must be deemed not to exist if it is not *informed*;
(ii) consent must be deemed not to exist if it is not *freely-given*;
(iii) consent must be deemed not to exist if it *bundled* in a manner that undermines the individual's interests;
(iv) consent must be deemed not to exist if the context is such that the individual has no meaningful *choice* available to them;
(v) all putative consent clauses that fail any of the above requirements must be prohibited, by means of *'unfair contract terms'* provisions;
(vi) these provisions must be *enforceable* in a tribunal or court, directly by individuals, including through 'test case', 'representative complaint' and/or class action processes, and by the relevant regulator(s).

Privacy consents often do not work

In contrast to what is proposed above, current practices fall far short. There has now been a great deal of research on consent and whether people can give effective consent and in what circumstances. The main research now concludes that people sign standard form contracts and privacy consents without reading them and consent is essentially illusory.[24] People almost never read privacy consents.[25] There are many examples of popular culture making fun of this ongoing systemic failure.[26] We all know that in practice the notice and consent model for privacy protection does not work.

The harm of continuing a privacy consent process when it is illusory

The harms for everyone in continuing to use privacy consent model, when it does not meet the above conditions, are serious and systemic.

- People are less likely to read privacy consents because it is well known that no one reads them. This just perpetuates the problem.
- Trust is eroded when people discover that they have consented to really unfair practices.
- People just get used to being exploited.
- People have no effective control over the use of their personal data.
- The model encourages and reinforces poor privacy practices and taking advantage of people because the business knowingly relies on illusory consent

Australia needs to act to stop this ongoing harm, .

[24] For example see *Beyond consent: improving data protection through consumer protection law* at https://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-through-consumer-protection-law

[25] See *94% of Australians do not read all privacy policies that apply to them- and that's rational behaviour* at https://theconversation.com/94-of-australians-do-not-read-all-privacy-policies-that-apply-to-them-and-thats-rational-behaviour-96353

[26] For example, South Park Episode Season 15 episode 1 – HUMANCENTiPAD where a cartoon character signs the latest iTunes update and is forced into a Group iPad experiment.

Unfair terms

In the consumer and financial services space there is now widespread acceptance that there may be "unfair terms" in all standard contracts. This is because the contract is written by and favours the business issuing the contract. Accordingly, there is now unfair terms legislation in place for all consumer and financial services contracts[27].

In the Final Report for the Digital Platforms Inquiry, the (then) Deputy Chair of the ACCC observed that "lacking a legal impediment and without fear of financial penalties, businesses have an incentive to include potentially unfair terms in their contracts".[28] The ACCC recommended (recommendation 20) that unfair contract terms are prohibited and not just voidable. This would mean that civil pecuniary penalties apply to the use of unfair contract terms in any standard form consumer or small business contract.

What needs to happen in the Privacy Act

A similar approach to unfair terms is needed for all privacy consents. That means there must be new provisions in the Privacy Act that deal with unfair terms for privacy consents. It must prohibit unfair terms, with civil penalties attached to the use of unfair terms. As in the unfair terms legislation there could usefully be a list of types of terms that will be considered unfair, but also give the regulator wide powers to prohibit further terms as unfair.

Further work is also needed to require all consents to be in plain language, with requirements of unbundled, clear and short consents. Guidance can be provided by OAIC once appropriate provisions are enacted

Standard terms

This review should seriously consider the scope for developing standard terms for privacy consents, to be utilised unless a business had good reasons for deviating from them. Once mature, these can be legislated, giving certainty for individuals and organisations. This would be a supplementary measure to dealing with unfair terms.

Independent research is also needed

The government needs to fund independent research into improving and testing how consents are delivered to people, to inform guidance that can be issued by the OAIC once the provisions are enacted. Testing is needed to check what works best so that consumers understand what they are agreeing to.

APF submits that:

(i) the onus of proof of compliance with all consent conditions should lie with the collector of the information;
(ii) separate consents should be required for each separate purpose ('unbundling' of bundled consents);
(iii) information for which consent is required should be unbundled from any information for which consent is not required (i.e. which is optional);
(iv) the 'related secondary purpose within reasonable expectations' test must also be tightened; and

[27] See for example, A guide to the unfair contract terms law at https://www.accc.gov.au/system/files/A%20guide%20to%20unfair%20contract%20terms%20law.pdf.

[28] Digital Platforms Inquiry Final Report page 497.

(v) the "take it or leave it" approach to consent and "bundled" consent should both be clearly interpreted as unfair terms.

Supporting details for these submissions are as follows:

- APF submits that tightening up the meaning of 'consent' alone will not be sufficient. It is also necessary to tighten up the wording in relation to collection necessity (APP 3.1-3.2), and use/disclosure for 'related' secondary purposes (APP 6.2(a)), in order to require companies to rely on genuinely free and informed 'consent' as the only legal basis for collecting, using or disclosing any personal information that is not strictly necessary to fulfil the original transaction (or otherwise required by law). Otherwise Facebook, Google and other companies will simply sidestep any new/stricter consent rules, either by defining their primary purpose in an overly permissive manner, or by arguing that their handling of personal information is 'related' to the primary purpose in some way as outlined in their privacy policy.

- The extraordinary breadth allowed under the 'related secondary purpose within reasonable expectations' test, given the OAIC's interpretation of APP 6.2(a) in dismissing a complaint about the deliberate release by Centrelink to the media[29] of the personal information of a welfare recipient, and particularly the personal information of her partner, demonstrates the inability of APP 6.2 to constrain even egregious behaviours.

- A further concern that needs to be addressed is the tendency of APP entities to adopt a 'take it or leave it' approach, and require consent as a non-negotiable term of contract. APF submits that consent to collection or use or disclosure of any item of personal information should only be accepted as a condition of use if the denial of consent can be demonstrated to undermine the provision of the service. The government should ensure that the "take it or leave it" approach to consent and "bundled" consent are both clearly interpreted as unfair terms which the ACCC can take action to remove under the unfair terms provisions in the Australian Consumer Law.

- Finally, the government should ensure that the effectiveness of consent is "consumer tested". Many consumers have been worn down and effectively trained to give consent as part of service provision. To ensure that consent is meaningful and not illusory it is necessary to independently test what consent is effective. When an effective method is designed then that design should be recommended as a standard.

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?

[29] See https://www.oaic.gov.au/media-and-speeches/statements/centrelink-debt-recovery-system#concluding-statement-centrelink-release-of-personal-information (currently unavailable due to website changes)

The existing protections are inadequate. Business is continually and as a matter of standard practice collecting more information than is reasonably necessary. This information is collected to get a data rich picture of people to be used for marketing purposes. That data is then sold to other businesses.

Specific guidance and rules are needed on the collection of unnecessary information.

To give an example of this problem we refer to Telstra's current practices in identifying their customers. Telstra is now in the practice of asking for a driver's licence as the main method of identification[30]. The problem with a driver's licence is that this is the most valuable piece of personal information for ID fraud.[31] In this way, Telstra exposes its customers to an unnecessary risk because they are asking for information that is not strictly necessary.

Another example, is buying a fridge at any retailer like The Good Guys, Harvey Norman or Bing Lee (but many others do this). This should be a straightforward transaction. Yet all of these retailers ask for personal information at the point of purchase. This is (misleadingly) under the guise of being able to claim on warranty or to get a receipt sent electronically. There is no explanation to the consumer on what happens to the information provided.

There are many other examples. People are misled into providing further information when it is unnecessary. They do not give genuinely informed consent and are not provided with any meaningful explanation.

The APPs are proving to be completely ineffective at protecting people. We recommend the Privacy Act legislate specific guidance on collecting unnecessary information with clear rules for businesses.

Our answer to the question in (a) above is 'No'. California's revised *Consumer Privacy Act* now includes 'A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title' (California Code 1798.125. (a) (1)). This would include refusal to provide unnecessary information. There is no direct GDPR equivalent, but Korean law includes such a provision. APF submits that the Privacy Act should include a provision such as the Californian anti-discrimination provision.

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

See our suggestions above. This needs to be the subject of further research and comprehensive testing of different forms of notice to inform guidance from OAIC in support of new consent provisions.

Exceptions to the requirement to obtain consent

31. What requirements should be considered to manage 'consent fatigue' of individuals?

See our suggestions above. This needs to be the subject of further research and comprehensive testing of different forms of notice to inform guidance from OAIC in support of new consent provisions.

Exceptions to the requirement to obtain consent

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

[30] See for example the Telstra complaint form at https://say.telstra.com.au/customer/general/forms/Email-Complaint.

[31] See https://www.abc.net.au/news/2019-09-06/drivers-licence-identity-theft-leaves-victims-exposed/11439668

The whole approach and 'device' of s 16A and 16B as separate exceptions that are just 'imported' into each APP as applicable, on the grounds that it makes the actual scope and effect of any APP almost impossible for a lay person to understand. This is an unacceptable approach to what is supposed to be consumer-oriented and citizen-oriented legislation. It makes the Privacy Act a 'known unknown' comparable to the obscurity of Singapore's data privacy legislation.

Pro-consumer defaults

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

In those situation where the OAIC can identify a clearly desirable default, APF supports OAIC have powers to determine standard terms and default terms.

Obtaining consent from children

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

Specific legislation is required for children. We suggest that the Attorney-General's Department specifically consult with the National Children's and Youth Legal Centre.

The role of consent for IoT devices and emerging technologies

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

One aim of 'principles-based' approach of the Privacy Act has been to retain 'technology-neutral'. There may need to be some specific legislative response to IoT issues, but this should not be due to specific technologies. APF endorses the submission by Burdon and Cohen ('4.4.1 Sensor Data Collections Are Different') on these issues, and in particular their stress that IoT/sensor data may produce inferred data that is personal data and possibly sensitive data. APF will address this in more detail in its response to the Discussion Paper.

Inferred sensitive information

36. Does the Act adequately protect sensitive information? If not, what safeguards should be put in place to protect against the misuse of sensitive information?

37. Does the definition of 'collection' need updating to reflect that an entity could infer sensitive information?

See our comments above on the importance of ensuring that inferred information is covered.

Direct marketing

38. 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?

Withdrawal of consent

39. Should entities be required to refresh an individual's consent on a regular basis? If so, how would this best be achieved?

APF submits that entities should be required to refresh consent on a regular basis. This would need to be focused on certain data sets. We would argue that where the customer is no longer using a service then there needs to be a mechanism to remind them after a reasonably short

period and obtain consent to retain the data (this will in any case be in the commercial or administrative interests of the APP entity). If consent is not provided/confirmed then the data should be deleted.

40. Should entities be required to expressly provide individuals with the option of withdrawing consent?

APF submits that withdrawal of consent should be a key right. If consent is given it must be able to be withdrawn, except in circumstances where an irrevocable action has already been taken which is inconsistent with withdrawal. This is consistent with the GDPR and subsequent laws in other countries.

The Privacy Act should specifically cover the withdrawal of consent and include:

- The right to withdraw consent
- Notice of the consequences of withdrawing consent
- If consent cannot be withdrawn in certain circumstances then an explanation of why not
- A process for the person to be able to obtain confirmation of deletion of the data once consent is withdrawn, unless retention is required by law.

41. Should there be some acts or practices that are prohibited regardless of consent?

APF agrees with OAIC's approach (see recommendation 40) that some information-handling practices should be fully or partially prohibited (irrespective of consent), and is has suggested five. We consider that these should be listed in the Act (and thus endorsed by Parliament). However, APF considers that (i) the Privacy Act should have a flexible provision allowing the Commissioner to prohibit additional practices by legislative instrument; (ii) the Act should set out the general criteria that the Commissioner must consider when making such a decisions, and procedures that must be followed; and (iii) the legislative instrument should be disallowable, so that there is Parliamentary input into the process.

Emergency declarations

42. 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?

APF does not have experience with this provision and does not make a submission.

Regulating use and disclosure

43. 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?

There is a need for prohibiting some uses and disclosure of personal information on the basis that they are exploitative or unfair. See our comments on 'use' above

3.7. Control and security of personal information

The Issues Paper fails to address a major innovation in the GDPR, 'demonstrable accountability' (GDPR art. 5(2)), a separate obligation on controllers over and above their specific obligations. However, the OAIC in Part 7 of is submission, 'Organisational

accountability requirements for entities', proposes detailed requirements for the demonstration of such accountability, and its relationship to data protection by design and default, privacy impact assessments, documented purposes, and privacy officers (recommendations 42-44).

APF endorses the OAIC's recommendations for demonstrable accountability. APF considers this is a major innovation in the GDPR, requiring active rather than passive compliance with good privacy practices, and that it would be a significant step in bringing the Privacy Act up to international standards.

However, APF does not endorse OAIC Recommendation 45 for a certification scheme. We discuss such schemes later.

Security and retention

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

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

The Act's security requirements date to the period 1980-2000. They are seriously inadequate in 2020, as demonstrated by ongoing and serious data breaches, and clear evidence of grossly inadequate policies, practices and technological features throughout business and government. The OAIC has had the opportunity to address the gap through its 'Guide to securing personal information'. It has failed to do so.

Most markedly, there is an almost complete absence of defined baseline security measures. The APF's submission to OAIC in 2013 provides further detail[32]. As a result, the necessary onus has still not been placed on organisations to either have that baseline in place, or have devised and implemented alternative designs that they can demonstrate by risk assessments to achieve at least the equivalent level of protection.

Access, quality and correction

46. 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

47. 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?

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

APF submits that any erasure rights should explicitly include a 'de-linking' right (sometimes called the 'right to be forgotten'). APF gives particular strong support to any rights of erasure not being limited in its scope to information provided by the data subject on the grounds of 'consent' in the first place.

[32] Australian Privacy Foundation Submission to OAIC of 7 January 2013, at https://privacy.org.au/Papers/OAIC-InfoSecy-1301.pdf

This broader erasure right is essential to a modern data privacy law. The European Union experience with the so-called 'right to be forgotten' pre-dates the 'erasure' right in GDPR art. 17, and originates in the *Gonzalez* decision of 2014.[33] In both pre- and post-GDPR, the right to 'de-linking' (and thus privacy through obscurity), or in some cases actual erasure, has been available to those whose personal data was collected without their consent, including under statutory authority. The overall experience in the EU has been positive, and data protection authorities and courts have been prudent in determining where use of the right is appropriate. APF submits that such a right, not limited to consent-based provision of data by data subjects, should also be adopted in Australia. Given the resistance of Australian courts to adopt any expansive interpretations of privacy protections (on the basis that law reform is a matter for legislatures informed by recommendations from a succession of law reform reports), the Government needs to ensure that any erasure right is worded so as to expressly incorporate a de-linking right such as adopted by courts in the EU. Because so much personal information is held on international platforms, internationally consistent jurisprudence is desirable, and this will be assisted by consistency in legislation across jurisdictions.

Establishment of such a right is constitutionally permissible and would not be contrary to recurrent High Court judgments about the implied freedom of political communication. We emphasise, consistent with EU jurisprudence, that consent should be substantive rather than merely formal.

3.8. Overseas data flows and third-party certification

49. What are the benefits and disadvantages of the current accountability approach to cross-border disclosures of personal information?

a. Are APP 8 and section 16C still appropriately framed?

The APF submits that the 'accountability' approach in APP 8 is unfit for purpose and should be repealed and replaced. APF therefore opposes OAIC recommendation 46, which proposes 'add ons' to APP 8 but leaves it otherwise intact.

There are many reasons why APP 8 should be repealed, six of which are set out here.

The use of 'disclosure' in APP 8 rather than 'transfer' probably means that there are no limits on international intra-company transfers of personal data under Australian law. This allows transfers to countries with no data protection laws, without imposing any additional requirements to ensure compliance by the foreign branch office (which may have no experience with privacy laws).

APP 8.1 allows a business to transfer personal data to anywhere in the world where the business (in its own assessment) has taken reasonable steps to ensure that the overseas recipient will comply with the APPs. It is then completely up to the data subject to find out that this has occurred, and to prove that the steps taken were not reasonable. This places an impossible and unfair burden on the data subject. The vicarious liability of the business for breaches committed by the overseas recipient (s. 16C) means little under such circumstances.

APP 8.2 is even worse because clause (a) completely exempts Australian businesses from compliance with APP 8 based on it merely holding a 'reasonable belief' that some overseas law 'or binding scheme' 'has the effect of protecting the information in a way that, overall, is at least substantially similar' to the APPs, and that there are enforcement mechanisms that 'the individual can access'. Apart from being ridiculously vague ('effect', 'overall', 'similar'), the

[33] *Google v AEPD & Gonzalez* (2014) CJEU

business only needs to hold a subjective 'reasonable belief' that this vague similarity exists, rather than this being an objective determination by a court or tribunal. Furthermore, the enforcement mechanisms only have to exist and be 'accessible' (according to the subjective belief of the Australian business), they do not even have to approximate the enforcement standards applying under Australia's law.

No 'white list' of overseas jurisdictions with 'substantially similar' laws was ever produced by the government despite its stated intention to do so.[34] This might appear to disadvantage businesses, but in fact disadvantages consumers, because they can never claim that a country was not a safe destination (the basis of a 'reasonable belief'), because it was not included on the government's 'white list'.

APP 8.2(c) is just as unfair, allowing businesses to justify transfers merely because of consumer consent, after being informed 'subclause 8.1 will not apply to the disclosure'. So, in order to protect themselves, consumers are expected to be fully informed about the implications of APP 8.1 and its interaction with the vicarious liability provisions of s. 16C. This ridiculous expectation is simply a blank cheque for data exports to anywhere, with no protections.

It is difficult to believe that a consumer could ever establish a breach of APP 8.1 or 8.2.

Neither APP 8.1 nor APP 8.2, nor the lacunae for intra-company transfers, meet international standards for international data transfers, such as the GDPR's 'adequacy' standard, and similar standards in many national laws. They are a major impediment to Australia obtaining a positive EU adequacy assessment, or similar assessments under other laws. They are a fraud on Australian consumers and citizens.

Australia cannot expect that the *Privacy Act* will have international credibility if these lax data export provisions are retained.

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

APF submits that if it is necessary to amend the Act to ensure that the decision of the Information Commissioner in *E v Money Transfer Service* is a correct statement of the law, the Act should be amended.

The more important point to be made about the extraterritorial application of the Act is that it is now too weak to protect Australians, in light of the enormous expansion of processing of personal data about Australians that takes place outside Australia, and may harm them. There needs to be added to the current provisions extra-territoriality based on overseas processing of data on Australians for the purposes of marketing to, or profiling of, persons within Australia by organisations outside Australia. This is the approach to extraterritoriality adopted by Europe in the GDPR, and increasingly found in very similar provisions in the laws of other countries.

APF submits that the extraterritorial provisions should be expanded to these marketing and profiling situations.

The OAIC's three proposals in recommendation 47 all expand the Act's extra-territoriality, and APF does not oppose them, but they are not as important as the reform discussed above.

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

[34] Australian Government, '*First stage response to the Australian Law Reform Commissioner Report 108*' (2009) 79.

APF submits that Australia should not under any circumstances be involved in the APEC-CBPR scheme ('APEC-CBPRs').

Deficiencies of APEC CBPRs have been documented elsewhere.[35] There are numerous 'challenges' to implementing CBPRs, which will only be summarised here.

(i) *The standards on which APEC CBPRs is based are the lowest standards of all international data privacy agreements.* APEC has endorsed the *APEC Privacy Framework*, a largely '1980s' standard based on the OECD Guidelines, as revised in 2013, but with some additional weaknesses, particularly its 'accountability' principle of allowing data exports subject to 'due diligence'. The Framework is the foundational standard on which the APEC CBPRs is based, standards well below those of the GDPR (or its predecessor, the Directive), or of Convention 108 (or its successor, '108+').

(ii) *Only three countries – not eight – participate fully in APEC-CBPRs*. In 2017-18 Australia and Taiwan were approved to participate in CBPRs. Mexico (2014), Canada (2014), and Korea (2016) obtained approval earlier. If and when any of these five countries appoint 'Accountability Agents' (AAs), then companies in their jurisdictions can apply to be certified as CBPRs-compliant. Until then, 'participation' in APEC CBPRs has no practical effect. None of these countries has yet appointed an AA. Canada called for applicants to be AAs in 2017.[36] It seems that some countries say they wish to participate in APEC CBPRs, and take preparatory steps, but then do not do so.

(iii) *Only a negligible number of companies are CBPRs certified.* Only three countries have appointed AAs:[37] the US (26 companies certified since 2013[38]), Japan (3 companies certified since 2016[39]) and Singapore (one company certified since 2019). So after six years of operation, APEC CBPRs only involves a tiny number (about 30) of US, Japanese, and Singaporean companies..

APEC economy	Approved to join APEC-CBPRs	Accountability Agent appointed	No. of Companies certified
USA	**2012**	**2013**	**26**
JAPAN	**2014**	**2015**	**3**
CANADA	2014	–	0
MEXICO	2014	–	0
KOREA	2016	–	0
SINGAPORE	2017	–	0
TAIWAN	2018	–	0
AUSTRALIA	2018	–	0
OTHER 11 IN APEC	–	–	0

[35] See G. Greenleaf, *Asian Data Privacy Laws*, 2014, pp. 33-37; Greenleaf, G., 'APEC's Cross-Border Privacy Rules System: A House of Cards?'(2014) 128 Privacy Laws & Business International Report, 27-30 <https://ssrn.com/abstract=2468782>; Greenleaf, Graham, Japan Joins APEC-CBPRs: Does It Matter? (December 1, 2016). (2016) 144 Privacy Laws & Business International Report, 18-21, Available at SSRN: https://ssrn.com/abstract=2964499

[36] See Gazette <http://www.gazette.gc.ca/rp-pr/p1/2017/2017-01-21/pdf/g1-15103.pdf > at p. 242.

[37] APEC CBPRs Accountability Agents listing < http://cbprs.org/accountability-agents/> .

[38] TrustAct *APEC CBPR Certified Companies* < https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list> as at 15 July 2019.

[39] See JIPDEC's APEC CBPRs Certified Companies list <https://english.jipdec.or.jp/protection_org/cbpr/list.html> (as at 15 July 2019).

(Singapore has since appointed an AA and certified one company)

(iv) *CBPRs-authorised transfers are an impediment to EU adequacy.* The European Commission states in its Decision concerning Japan's adequacy assessment that certification of a company as APEC CBPRs compliant cannot be the basis for any onward transfer of EU-origin personal data from a country that is held to be GDPR-adequate.[40] This will further diminish the business case for CBPRs.

(v) *CBPRs is therefore of negligible practical significance.* The only beneficiary being a handful of US companies which Japanese and Singaporean laws allow to be the recipients of personal information.

(vi) *There is no business case for any Australian company becoming CBPRs-certified*. Australian companies are required to comply with the *Privacy Act*, which has higher standards than APEC-CBPRs, so why would any company outside Australia find it at all relevant that an Australian company is also CBPRs-certified.

The only purpose that would be served by Australian participation in CBPRs would be to further appease the United States, which is not a good basis for policy. Australia can continue to pretend to participate, but should do nothing further.

APF submits that developing a 'CBPRs Code' under Part IIIB of the Act would be an expensive waste of money, time, and policy focus, all of which can be better spent on other improvements to the *Privacy Act*. No Australian business would gain any benefits from the availability of such a Code, and in all probability none would make use of it (as in three current participating countries).

APF therefore strongly opposes the OAIC's ridiculous proposal (recommendation 45) that a domestic certification scheme 'be interoperable the APEC CPBR system'. It is ridiculous because the standards for APEC-CBPRs certification are so much lower than the standards for compliance with the Privacy Act (particularly if any of OAIC's proposed reforms are enacted!), that there can be no 'interoperability', consistency or any other compatibility. APEC-CBPRs is a 1980s era privacy standard, whereas the Privacy Act aspires to be a standard for the 2020s.

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

APF submits that a certification scheme should not be 'in addition' to APEC-CPBRs, because (as stated above), Australia should not be involved in APEC-CPBRs at all, under any circumstances. APF submits that such certification schemes must be developed with considerable care to avoid the problems mentioned below, but is not completely opposed, just sceptical, about certification being used as a means of implementing 'demonstrable accountability' (in GDPR terms). However, APF's overall view is that such a scheme is a very low priority in relation to Privacy Act reforms.

Privacy 'seals', 'badges' and certification have had a poor track record elsewhere, due largely to their capture by industry and with the result that data subjects are misled that their personal information is safe. These dangers are exacerbated by two factors. There is an inherent conflict of interest involved when the certifying organisation depends on revenue flowing from those it certifies (and particularly from renewals of certification), so that where

[40] [European Union] Commission Implementing Decision of 23.1.2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information < https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf >

it refuses/revokes certification, it is closing down its own revenue flows. Where certification is voluntary, then the certifying body has to sell the idea of certification at all, which is likely to involve implied promises that certification is easy to obtain (otherwise, why would companies risk losing money on failed certification attempts).

The government will need to avoid these dangers if it proposes a certification scheme. If a scheme required certain businesses to be certified, this compulsion might remove many of the above problems with both initial certification and re-certification. It is also important that the OAIC is not certifying businesses itself (but only approving certification agents who are to carry out the audits), because otherwise the OAIC would have a conflict of interests when investigating alleged breaches by certified companies. To deal with other possible conflicts concerning appointment of auditors, we recommend the introduction of objective criteria for certifying auditors, and that they should be subject to periodic performance reviews by the OAIC.

Another difference from APEC-CBPRs certification is that the certification bodies would be certifying against compliance with the *Privacy Act*. In contrast APEC-CBPRs 'Accountability Agents' such as TrustArc only certify against the far lower standard of the APEC Privacy Framework, not against the standard of national laws of the companies certified.[41] These inconsistent and irreconcilable standards for certification means that the two should not be mixed.

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

APF submits that Australia's long-term interests, and in particular the interests of Australian businesses, would be well served by Australia strengthening its privacy laws sufficiently to allow Australia to obtain a positive adequacy assessment from the EU under its General Data Protection Regulation (GDPR).

Japan has obtained a positive EU assessment in 2019 (to be reviewed in 2021), New Zealand did so in 2013 (also to be reviewed in 2021), and Korea is likely to do very shortly. All three of these significant trading partners of Australia's have amended their laws in the past year, making them more amenable to EU adequacy considerations in the process. Canada is going through the same process, as its current adequacy finding is also to be reviewed in 2021.

One consequence of these Asia-Pacific countries being regarded by the EU as providing adequate protection is that they must not allow unrestricted transfers of personal information (including personal information originating in the EU) to be transferred to countries (such as Australia) which do not provide similar adequate protection. Transfers from any of these countries to Australia will thereof have to be considered on a case-by-case basis, and protected by contractual means, resulting in higher compliance costs than if Australia was simply regarded as another 'adequate' destination.

If Australia did satisfy EU adequacy requirements, Australian businesses would then be able to receive personal data from companies in the EU, without the necessity for any special arrangements in relation to individual transactions. Many Australian companies are already aiming to comply with the GDPR in order to satisfy the requirements of head offices based in the EU or elsewhere, or as a requirement imposed on contractors in the supply of services

[41] Greenleaf, G, 'APEC's Cross-Border Privacy Rules System: A House of Cards?' (2014) 128 *Privacy Laws & Business International Report*, 27-30 https://ssrn.com/abstract=2468782

provided to the EU. Given that there is already significant 'GDPR creep' in Australia, a formal finding of adequacy in relation to Australia would reduce these compliance burdens on Australian companies, as well as increasing protections for Australian consumers. [42]

One 'disadvantage' (but of benefit to Australian consumers and citizens) is that it would be necessary to better protect privacy of Australians against exports to jurisdictions with non-adequate regimes, than is currently the case under APP 8 (which, as submitted above, should be replaced).

To facilitate the EU finding Australia's protections to be 'adequate', Australia should also apply to accede to data protection Convention 108+, in accordance with Recital 105 of the EU GDPR. Although Australia has been an Observer on the Consultative Committee of Convention 108 since the 1980s, it does not attend meetings of the Committee, and thus does not contribute to the ongoing development of the procedures and standards under which the 'modernised' Convention 108+ will develop. The APF is accredited as an Observer to this Committee, and does participate. Participation by the Australian government (or the OAIC) would assist the government to be better attuned to the development of international data privacy standards, and Australia would benefit by eventually becoming a party to the Convention.[43]

APF submits that Australia should have the objective of becoming a party to Convention 108+.

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

54. Is the current enforcement framework for interferences with privacy working effectively?

APF submits that the current enforcement framework is not working effectively. The provision of sufficient resources is only part of the reason why the Privacy Act and the OAIC have been so ineffectual, arguably dysfunctional, for privacy protection for so long. Another major reason is that Courts and Tribunals have had so few opportunities to interpret the Privacy Act, and its enforcement, and thus to instruct the Privacy Commissioner on how the Act must be interpreted and enforced. Part of the reason for this is that successive Commissioners' actions have contributed to keeping complaint decisions away from the AAT and the Courts.

Although the *Privacy Act 1988* has been in force for 30 years, only a handful of non-trivial cases have been decided by the Courts. The relatively recent inclusion in the *Privacy Act* of the s96(1)(c) right of appeal against s52 Determinations by the Commissioner[44] should have allowed AAT and court decisions to shine some light into corners of the Act. However, this has not occurred, because (put bluntly) successive Privacy Commissioners have refused to make s52 Determinations. The track record of all Commissioners to 2014 was that, on average, not even one person per year would obtain a s52 determination, so that they could consider appealing against it. [45] For 2011-14 the average was two per year.[46] From 2014-18 the

---

[42] G. Greenleaf "'GDPR Creep' for Australian Businesses But Gap in Laws Widens" (2018) 154 *Privacy Laws & Business International Report* 1, 4-5, <https://ssrn.com/abstract=3226835>

[43] G. Greenleaf 'Balancing Globalisation's Benefits and Commitments: Accession to Data Protection Convention 108 by Countries Outside Europe' (June 23, 2016). *UNSW Law Research Paper No. 16-52*, <https://ssrn.com/abstract=2801054>

[44] *Privacy Amendment (Enhancing Privacy Protection) Act* 2012, in force 2014.

[45] Greenleaf, G, 'Privacy Enforcement in Australia is Strengthened: Gaps Remain' (2014) 128 *Privacy Laws & Business International Report* 1-5 https://ssrn.com/abstract=2468774 ;

[46] Numbers of Determinations for 2011-14 were: 5 (2014); 0 (2013); 1 (2012); 1 (2011); Source: OAIC <https://www.oaic.gov.au/privacy-law/determinations/Page-4#pagelist> ; figures for earlier years can be found from the AustLII website.

average has risen to 5.5 per year,[47] but this still represents less than one appealable decision every two months. In 2018-19 there were 3 Determinations. Furthermore, these are something close to 'self-selected' complaints, the ones that the Commissioner has 'let through' to the Determination stage, as explained below, and the results of the Determinations are overwhelmingly in favour of complainants, with breaches of the Act being found, and some type of remedy being awarded (compensation or otherwise). So it is perhaps not surprising if (on the most positive figures), where there are an average of 5 successful complainants out of 5.5 Determinations per year, the 0.5 Determinations where no breach is found do not generate many appeals to the AAT or the Courts. But why are there so few negative Determinations?

A major reason for the lack of negative Determinations has been that successive Commissioners have insisted that they will dismiss complaints if they think 'the respondent has dealt adequately with the complaint' (s41(2)(a)), even though the complainant disagrees that they had been dealt with 'adequately'. Alternatively, Commissioners have claimed that there has been 'no interference with privacy' (s41(1)(a)), even in cases where the facts were not in dispute, but interpretation of the law and its application to those facts was contested between the parties. Other sub-sections of s41 also give the Commissioner wide discretions not to investigate complaints.

It appears from anecdotal reports that the Commissioner insists on such dismissals even where the complainant states that they wish to have a formal Determination made, and even in cases where the complainant is seeking a formal Determination in order to test the law, because the matter is of public interest rather than simply about their own private right to privacy. Such dismissals block dissatisfied complainants obtaining s52 determinations, and thus block the right of appeal to the AAT, and eventually to the courts. The result is that AAT and the courts have close to non-existent opportunities to consider the Commissioner's interpretations of the Privacy Act, or the appropriateness of remedies under it. The application of the law is thus opaque, and as a result can have unfair consequences, but without adequate recourse to review of the OAIC's decisions.

APF therefore submit that the Government should remove at least the s41(1)(a) and s41(2)(a) impediments to s52 determinations, by amendment to the sub-section to provide that, if a complainant objects to the Commissioner's dismissal of a complaint under these sub-sections, the Commissioner will then make a formal determination under s52. This will give complainants (and respondents) the opportunity to appeal to the AAT.

This important issue is completely absent from the Issues Paper, other than for the oblique comment that 'There is currently no requirement for the Commissioner to make a determination where a complaint is not resolved by conciliation, nor is there a right of a party to require a determination in such circumstances.' No justification for these provisions is given. APF submits that this issue should be given detailed consideration in the Discussion Paper, and that APF's suggested amendment should be adopted.

Such an ability to obtain a Determination and an AAT hearing continues to be justified once a direct right to enforce the Privacy Act (see below) is introduced. A complainant who has commenced seeking redress via a complaint to the Privacy Commissioner, rather than going direct to the court, should not be forced to 'start again' if the Privacy Commissioner is not

[47] Numbers of Determinations for 2015-18 were: 3 (2018); 5 (2017); 9 (2016); 5 (2015); Source: OAIC <https://www.oaic.gov.au/privacy-law/determinations/Page-4#pagelist > as at 6 February 2018. It is possible that the OAIC has failed to yet list some Determinations since March 2018 (the most recent Determination recorded), but there is no source of information other than the OAIC's website, so if there are more Determinations not yet listed, this is another 'transparency gap'.

willing to further investigate their complaint, they should have the opportunity to go to the AAT.

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

The current Australian Consumer Law (ACL) maximum penalties are the highest of A$10 million, or three times the benefit received, or 10% of the turnover of the business. The Government had proposed such an increase, noting that the 10% is calculated against local annual turnover. APF submits that if Australian privacy law is to have a deterrent effect on global companies of the scale of Google and Facebook, the maximum fines that can be issued should be proportional to the global turnover of the company concerned,

While any increase in penalties for breaches of the *Privacy Act* will be an improvement on the current situation, APF does not consider that parity with the penalties for breaches of the Australian Consumer Law is the appropriate standard. APF submits that the preferable standard for higher penalties for breach of the Privacy Act is that set by the European Union's *General Data Protection Regulation* (GDPR) so that, depending on which provisions have been breached, there can be a fine of 2 to 4% of the 'total annual worldwide turnover' of a company, or a fine of 10 to 20 million euros, whichever is the higher (GDPR art. 83(4)-(6)).

Since January 2019 administrative fines have been issued with increasing frequency under these GDPR provisions. Examples include fines by France's CNIL against Google (€50 million), UK Information Commissioner's against British Airways (£20M) and against Marriott hotel chain (£99M proposed, not yet finalised) for major data spills, by the German DPA against H&M retailers (£31M), and by the Irish DPA against Twitter (€450,000),

This 'EU benchmark' of '2-4%' is being reflected in Bills in the process of enactment in many countries. It has been proposed in India. It has already been enacted in Korea, at the level of 3% of global annual turnover. One fine of US$4.5 million (approximately) was issued against a shopping mall for a data breach, and in November 2020 a fine of US$6M against Facebook. Fines of this level are no longer restricted to Europe, they occur in the Asia=Pacific, and Australian regulators also need that capacity.

As things stand, a small penalty will be accepted by leading platform operators and their partners as an acceptable cost of business, one that does not tangibly affect their profitability, does not result in disinvestment, that does not gain the attention of the mass media and that does not meaningfully erode the operator's social licence. Meaningful penalties are consistent with recurrent calls by the ACCC for higher penalties to influence corporate behaviour. They are also consistent with the conclusions of the Royal Commission into Misconduct in the Banking, Superannuation & Financial Services Industry.

56. Are the remedies available to the Commissioner sufficient or do the enforcement mechanisms available to the Commissioner require expansion?

a. If so, what should these enforcement mechanisms look like?

APF submits that another potent form of deterrent, particularly applicable to data privacy breaches, should be introduced: statutory damages should be able to be awarded to all persons whose personal data was disclosed as a result of a data breach due to negligent security (or other reasons in breach of the law), with a statutory penalty able to be awarded of up to a limit (in South Korea, it is 3 million won or US$3,000) per person to a class of those whose data was leaked, without need for claimants to prove actual damage.

The potential liability resulting from a $3,000 statutory liability, for even a data breach of sensitive data of one million individuals could amount to 3 billion dollars. Some data breaches involve millions of individuals, and they often include biometrics, ID numbers and other most sensitive information. The relevance of statutory damages to the ACCC's deterrent objectives is that the risk of imposition of such damages can convert data which platforms (or their surveillance market customers) consider valuable only because of its surveillance marketing uses, into potentially toxic data, and thus deter companies from retaining it beyond when its necessary uses have expired. A properly framed damages provision, where the purpose for which data was retained is one of the contributing factors to the quantity of the per capita damages, could be a powerful deterrent. Statutory damages following from a private right of action are also included in California's new California Privacy Rights Act of 2020, but only for breaches of the security principle.

3.10. Direct right of action

57. 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?

APF gives strong support to a direct right of action under the Act, both because an alternative enforcement route will benefit complainants, and because is that it will mean that Courts will have the opportunity to interpret the *Privacy Act*, and Courts will through their judgments set standards for what are appropriate types and levels of penalties and compensation for privacy breaches. APF's detailed reasons are as follows:

APF gives strong support to this Recommendation. It is crucial that individuals can seek access to justice when there has been an interference with their privacy. To provide meaningful access to justice there must be two paths available: (i) access to Court to seek compensation and other orders; and (ii) access to an alternative free dispute resolution scheme (which is the OAIC). It is essential to have both options because many people cannot afford to go to Court, but must be able to seek compensation without needing to do so. However, the investigation and enforcement functions of the Privacy Commissioner have operated in a very unsatisfactory manner for many reasons (some of which are discussed below), only some of which can be addressed by providing more resources to the OAIC. It is therefore of equal importance to allow direct access to the courts to those who wish to take that route to obtain compensation, and have the means to do so.

APF notes that the Law Reform Commissions of at least the Commonwealth, NSW and Victoria have published detailed analyses and Recommendations to this effect in 2008, 2009 and 2010 respectively, alongside recommendations by parliamentary inquiries. Those recommendations are practical, and have not been opposed by consensus bodies such as the Law Council of Australia.

Where individuals have sufficient resources to take a breach of the Privacy Act before the courts, without need to first complain to the OAIC, there are very good reasons to enable them to do so, including practical reasons such as: (i) where plaintiffs are willing to fund their own litigation, with the risk of the award of costs against them, this is one indicator of the seriousness of a complaint; and (ii) where cases go before the courts, this may reduce the costs to the OAIC of complaint investigation and enforcement actions.

However, the most important reason for supporting an alternative enforcement route is that it will mean that Courts will have the opportunity to interpret the *Privacy Act*, and Courts will

through their judgments set standards for what are appropriate types and levels of penalties and compensation for privacy breaches. The APF notes the importance of the transparency provided by both litigation and by engagement with professional and other communities. A key weakness of the OAIC regime under the *Privacy Act 1988* is that agency's ongoing emphasis on closed-door complaint resolution, and its resistance to disclosure of how it makes decisions in response to complaints. Such resistance is ironic given the OAIC's role as the Commonwealth's freedom of information agency and the strong desire across both industry and civil society for information that will enable stakeholders to understand how the OAIC is interpreting the Privacy Act. Litigation would provide the sunlight that is the best disinfectant for administrative inefficiency and consumer exploitation. It offsets the disquiet among consumers evident in empirical research about the timeliness and sufficiency of the OAIC's handling of complaints.[48] It would help provide the certainty that business expects in dealing with consumers, governments and other enterprises.

The Australian practice that, in most cases, 'costs follow the event' in litigation will have the effect of 'balancing the need to appropriately direct court resources', because the possibility of costs against will deter litigants who do not have a meritorious claim.

Another approach to providing a direct right of action to enforce the *Privacy Act* is proposed by Salinger Privacy in its submission (pp. 36-37), as access to a 'a tribunal which defaults to no-costs basis hearings', subject to the complainant first having sought an informal resolution, and with a limit on damages available ($150,000 suggested). Salinger argues that 'NSW offers a model for accessible justice in relation to privacy complaints':

> Since the *Privacy and Personal Information Protection Act 1998* (NSW) commenced in 2000, there have been over 460 privacy cases reported. While by no means a perfect system, the NSW Civil and Administrative Tribunal offers complainants an opportunity to be heard, without needing legal representation or being exposed to costs orders. Cases may only be lodged if the complainant has first sought an 'internal review' by the respondent, and either the internal review was not completed within 60 days, or the complainant was dissatisfied with the result. The NSW Privacy Commissioner is notified of each internal review, and has the right to appear as *amicus curiae* in the Tribunal. The vast majority of cases which result in compensation are at the low end of the scale, typically less than $10,000.

APF has no objection to a direct enforcement right being to such a tribunal, rather than a court, provided there is a right of appeal from the tribunal to the court system. This is essential so that judicial interpretations of the Privacy Act can develop.

APF endorses OAIC recommendation 51 that the direct right of action must not be limited to 'serious' breaches of the Privacy Act. It should be available in relation to any 'interference with privacy'. APF also endorses OAIC recommendations 54, 55 and 56, each of which will significantly strengthen the operation of the direct right of action.

However, APF strongly rejects OAIC recommendation 52 that individuals should be required to make a complaint to the Privacy Commissioner before utilising their right to apply to the courts. There should be no such requirement. It is a proposal, because the principal reason why the direct right of action is needed is because of widespread dissatisfaction with how the OAIC handles (or fails to handle) privacy complaints: they take six months or more to even start considering a complaint; they use multiple means of disposing of complaints without

[48] See for example Jodie Siganto and Mark Burdon, 'The Privacy Commissioner and Own-Motion Investigations into Serious Data Breaches: A Case of Going Through the Motions?' (2015) 38 (3) *University of New South Wales Law Journal* 1145

making a decision (determination); they will not make negative determinations at the request of complainants; the amounts of damages awarded are derisory.

What OAIC needs to help shake it out of its lethargy is some regulatory competition from the courts (or tribunals, as Salinger Privacy suggests). What the Privacy Acts needs is Courts or Tribunals making decisions on the appropriate levels of damages or other remedies for particular interferences with privacy, and making decisions which interpret the Act with the force of law behind their decisions. Only then will the OAIC have proper directions on how to carry out is job.

The APF also strongly rejects OAIC recommendation 53 that they should be given power to refuse to investigate complaints where, in the OAIC's opinion, 'the matter is more appropriately dealt with by the courts'. Such powers would make the 'direct right of action' (for complainants) into a travesty: it would become instead a right that the OAIC has to refuse to carry out its duties under the Act, and instead force complainants, wherever it does not like a complaint, to take the matter to court instead (whether the complainant wants to or not). Many, perhaps most, complainants cannot afford the costs involved in initiating court actions.

OAIC is 'trying to have two bob each way': it wants to insist that all complainants start by complaining to it, rather than going to court; and then it wants the compel whichever complainants it does not like to go to court, whether they want to or not. Both these ridiculous recommendations (52 and 53) should be rejected.

3.11. Statutory tort

58. Is a statutory tort for invasion of privacy needed?

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

60. What types of invasions of privacy should be covered by a statutory tort?

61. 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?

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

63. 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?

APF gives strong endorsement to a statutory tort for invasion of privacy, of the type recommended by the Australian Law Reform Commission (ALRC). The ALRC's examination of the need for a statutory cause of action for serious invasions of privacy was very thorough and its recommendations well-balanced. The recommendation has been supported by all relevant inquiries that have considered this issue, and is a long-overdue reform that fills a glaring gap in the law.[49]

The Australian Privacy Foundation made submissions[50] to the ALRC during its enquiry which were stronger at various points than the ALRC's final recommendations. A NSW

[49] ALRC (2008) 'For Your Information: Australian Privacy Law and Practice' Report 108, Australian Law Reform Commission, August 2008; NSWLRC (2009) 'Invasion of Privacy' Report 120, August 2009; VLRC (2010) 'Surveillance in Public Places', Victorian Law Reform Commission, August 2010.

[50] Australian Privacy Foundation 'Serious Invasions of Privacy in the Digital Era' Australian Privacy Foundation Submission to the Australian Law Reform Commission https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2360928

Parliamentary Committee also recommended in 2016 a statutory cause of action[51] which went further than the ALRC recommendations (which were confined to intentional or reckless conduct), and proposed that corporations (and government) should also be liable for negligent conduct which otherwise met the criteria for the statutory cause of action. The Government should examine both the APF submission and the NSW report, and consider strengthening its recommendation accordingly. APF notes that there has been a succession of other reports recommending establishment of a statutory cause of action. While the introduction of a privacy cause of action has historically been opposed by media organisations, such development is consistent with the implied freedom of political communication and, as evidenced by experience in comparable jurisdictions with private causes of action, would not impermissibly encumber the operation of established or emerging media organisations. The ACCC correctly argued that the impact on freedom of speech, and on media operations, will be minimal (pp. 494-5).

The APF's view is that the recent developments in law noted in the Issues Paper, while welcome, are very partial, and they in no way negate, or even reduce, the need for the establishment of a tort of privacy on a policy basis.

We also strongly believe that the diversity and complexity of the privacy interest is such that the specification of objective tests is infeasible, particularly while no jurisprudence exists.

Further, APF submits that the scope of the right must extend beyond intentional invasions of privacy to also include reckless or negligent behaviour. We note that OAIC recommends likewise (recommendation 60).

APF supports OAIC recommendation 60 that it should be notified of 'serious invasion of privacy cases', and have the right to intervene in such proceedings, or act as *amicus curiae*.

The APF's view is also that it is highly desirable that the privacy right of action be clearly defined as a statutory tort, in order to embed it within an established branch of law.

The APF's longstanding policy[52] remains in place:

1. it must available to individuals, but not to legal persons such as companies
2. it must enable a court to grant injunctions, award damages, and impose penalties exemplary or punitive damages
3. it must require the court to balance the privacy interests of the litigant against other important interests, including and especially 'the public interest'
4. it must provide a clear framework and criteria for evaluating a defence that an invasion of privacy is justified in the public interest

We also draw attention to the APF's Policy Statement on 'Privacy and the Media'[53], which includes 'Guidelines' on what we believe to be an appropriate interpretation of the public interest.

Salinger Privacy's submission (p. 38-39) provides good reasons why conduct which is exempt under the Privacy Act should not be exempt from a 'serious invasion of privacy' claim.

---

[51] https://www.parliament.nsw.gov.au/lcdocs/inquiries/1877/Report no 57 Remedies for the serious invasion of .pdf

[52] https://privacy.org.au/policies/right-of-action/

[53] https://privacy.org.au/policies/media/

The proposed right of individual direct enforcement of the Privacy Act is a necessary complement to the statutory action for serious invasions of privacy. APF gives strong support to both reforms being enacted. The two are not the same, because (i) a breach of the Privacy Act might not constitute a 'serious invasion of privacy', but the Act nevertheless allows a remedy; and (ii) not all of the defences available to a claim of serious invasion of privacy (eg public interest) will be available in relation to a breach of the Privacy Act.

3.12. Notifiable Data Breaches scheme – impact and effectiveness

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

65. Has the NDB Scheme raised awareness about the importance of effective data security?

66. 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?

The frequency and severity of data breaches, by both private sector and public sector entities, is increasing constantly. The effectiveness of the NDB scheme depends to a large extent on the severity of administrative fines and other penalties that entitles come to expect for both (i) failure to comply with the NDB scheme; and (ii) the data breach itself (usually but not always a breach of the security principle). In Australia these penalties are, in practice, no where near severe enough.

APF supports OAIC recommendations 62-66 concerning both the NDB scheme, and the underlying data breach.

3.13. Interaction between the Act and other regulatory schemes

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

68. Is there a need for greater harmonisation of privacy protections under Commonwealth law?

a. If so, is this need specific to certain types of personal information?

Mandatory data breach notification is not yet required in every State and Territory law in Australia. APF submits that obtaining such consistency should be a priority for harmonisation.

69. Are the compliance obligations in certain sectors proportionate and appropriate to public expectations?

In principle, we cannot see any reason to repeal privacy related provisions in other legislation, or to generally oppose new specific provisions where appropriate. It will often be possible in sectoral legislation to be more specific about necessary and therefore permissible collection, uses and disclosures, and thereby offer individuals greater safeguards and assurances.

4. Additional submissions

APF notes the need for coherent, effective and forward-looking consumer protection in dealing with global digital platforms such as Facebook, Google and Amazon and local platforms whose business practices are founded on what has been characterised as Surveillance Capitalism. The regulation of practices that erode privacy is a key aspect of that protection, highlighted in a range of international reports such as the US Congress 2020 report on digital platforms and authoritative work by researchers such as Kemp's 2020

'Concealed Data Practices' study.[54] A broad range of government, commercial, civil society and scholarly investigations have demonstrated the need for an integrated approach to privacy – and more broadly data – protection, addressing the regulatory balkanisation that confuses consumers, enables exploitation by private/public sector entities, fosters incapacitation on the part of regulators and fails to address emerging issues such as under-disclosure by global corporations engaged in the commercialisation of genomic data.[55]

That balkanisation is being exacerbated in Australia through the proliferation of overlapping but typically under-resourced regulators at the national and state/territory levels, for example the Office of the National Data Commissioner (with oversight by the Commonwealth Ombudsman), the Office of the Australian Information Commissioner, the National Health Practitioner Ombudsman & Privacy Commissioner, Australian Communications & Media Authority and the Australian Competition & Consumer Commission.

A coherent framework for privacy, centred on a strengthened Privacy Act that its not vitiated by an incapacitated and under-resourced Office of the Australian Information Commissioner and by the proposed Data Transparency & Availability regime,[56] will strengthen national and international competition policy – highlighted in for example the ACCC 2019 *Digital Platforms* report – and give effect to protections against unfairness under the Australian Consumer Law and jurisprudence dealing with unconscionability.

APF endorses in particular recommendations in the ACCC *Digital Platforms* report regarding amendments to the *Competition and Consumer Act 2010,* discussed below. Adoption of those recommendations will align Australia with the European Union and Californian law (two best practice benchmarks) and have a very significant effect on the protection of privacy in relation to businesses adversely affecting privacy. The reforms will strengthen the necessary role of the ACCC in the protection of privacy, a role that has been welcomed by civil society and regulatory analysts alike on the basis of principle and the ACCC's proactive stance. APF supports both recommendations, and regards them as central to the privacy reform agenda.

4.1. Prohibition against Unfair Contract Terms

In highlighting information asymmetries in the interaction between consumers and digital platforms (and more broadly between many businesses and consumers, including the financial institutions whose unconscionable behaviour was condemned in the Hayne Royal Commission)[57] APF submits that unfair contract terms should be prohibited rather than merely voidable. That prohibition should, as recommended by the ACCC, have a statutory basis under the Competition and Consumer Act 2010 and be accompanied by stronger civil pecuniary penalties to ensure sufficient deterrence. Regulatory scholars, the ACCC, the Productivity Commission, law reform commissions and parliamentary committees have noted

[54] Katharine Kemp, 'Concealed data practices and competition law: why privacy matters' (2020) *European Competition Journal* (in publication)

[55] See for example Bruce Baer Arnold and Wendy Bonython, ''Not As Good as Gold: Genomics, Data and Dignity' in Monique Mann, Kate Devitt and Angela Daly (eds), *Good Data* (Institute of Network Culture, 2019) 135; and Wendy Bonython and Bruce Baer Arnold, 'Privacy, Personhood, and Property in the Age of Genomics' (2015) 4(3) *Laws* 377

[56] APF draws attention to submissions regarding the *Data Availability & Transparency Bill 2020* (Cth), noting that the legislation in practice will serve to fundamentally erode privacy protection by authorising sharing of personal data across Commonwealth government agencies for a wide range of purposes, will enable sharing with non-government research entities and will potentially allow sharing with commercial entities without adequate supervision. That is of particular concern given the mandatory nature of data collection and substandard data protection practice within public/private sector bodies including leading universities and government agencies.

[57] Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry

that inadequate penalties are shrugged off as an acceptable cost of doing business and do not foster changes to corporate culture.

It is fundamental that the ACCC should be able to hold digital platforms and other businesses to account for unfair contract terms. APF endorses the ACCC's assessment that 'This is particularly significant in standard form contracts where there is a zero monetary price, like many digital platforms' terms of use and privacy policies, where the impact of declaring a term void is less likely to have immediate impacts on the parties' financial rights and obligations. Introducing penalties to the use of UCTs will help lessen the bargaining imbalance between businesses and consumers regarding privacy policies.'

4.2. Prohibition against certain unfair trading practices

ACCC recommended that the Government amend the *Competition and Consumer Act 2010* (Cth) to expressly prohibit certain unfair trading practices *not currently caught by the consumer protection laws but have the potential for significant consumer harm*. Those practices include businesses:

- collecting and/or disclosing consumer data without express informed consent
- failing to comply with reasonable data security standards, including failing to put in place appropriate security measures to protect consumer data
- unilaterally changing privacy provisions in the terms on which goods or service are provided to consumers without reasonable notice, and without the ability for the consumer to consider the new terms, including in relation to subscription products and contracts that automatically renew
- inducing consumer consent or agreement to data collection and use by relying on long and complex contracts, or all or nothing click wrap consents, and providing insufficient time or information that would enable consumers to properly consider the contract terms
- engaging in practices that seek to dissuade consumers from exercising their contractual or other legal rights, including requiring the provision of unnecessary information in order to access benefits."

APF has recurrently highlighted the authority to deal with unfair practices found in overseas regimes such as in the EU, UK, USA, Canada and Singapore. Adoption of the prohibition against unfair practices is administratively viable, addresses the inadequate self-regulation of leading digital platforms and other businesses, and will serve to align Australian law with the EU and North America. It will foster consumer trust and enabling Australian regulators to benefit from experience in other jurisdictions in regulating what will often be the same online platforms.

3.3 Privacy Impact Assessments (PIAs)

This topic appears not to be mentioned in the Review. PIAs lie at the very heart of privacy protection. The ongoing, very low grade of both substantive and procedural compliance with the public's expectations and needs for privacy protection, by both government agencies and corporations, results in ill-informed designers, unjustifiably privacy-invasive designs, widespread disillusionment with the sponsors of information systems and with the law's inability to protect the public, sullen opposition, low returns on investment, and project failures.

APF submits as follows:

- PIAs are more often than not conducted too late in a project timeline, after key policy and design features have already been decided, rather than earlier when they can usefully inform choices between alternatives, allowing 'privacy by design'.
- PIA processes are routinely devised in order to avoid engagement with either the public directly or with representatives of and advocates for the public interest;
- even where some degree of engagement is undertaken, vital information about the design is often suppressed;
- the scope of PIAs is in many cases intentionally limited to much less than the full project, with the effect that an overview of schemes' privacy impacts and implications is prevented, and features turn out to have very different impacts from what was apparent from partial studies;
- PIA Reports are commonly suppressed, or their publication delayed, or their availability not communicated to the parties interested in engaging on the matter;
- major changes are made to designs, with significant privacy implications, but without notice to the relevant organisations, and without the requisite re-working of the PIA or commencement of a new PIA process.

APF submits that firm and clear requirements must be imposed on agencies and corporations, to conduct PIA processes, to conduct effective processes, to engage the real stakeholders i.e. those who are affected by the measure, to reflect the points made by stakeholders during the PIA process, and to make information and reports available to the stakeholders in a timely and convenient manner.

Australian Privacy Foundation – Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, Committees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby and Elizabeth Evatt, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-) http://www.privacy.org.au/Campaigns/Media/