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*

Graham Greenleaf, David Lindsay, Bruce Arnold, Roger Clarke, Katherine Lane, Nigel Waters & Elizabeth Coombs[1] – on behalf of the Australian Privacy Foundation.
10 September 2019

[1] Graham Greenleaf AM is Professor of Law & Information Systems at the University of New South Wales;; Dr Bruce Arnold is Assistant Professor, School of Law & Justice, University of Canberra; David Lindsay is Professor of Law, University of Technology Sydney; Roger Clarke is Principal, XamaX consultancy, and Professorial Visiting Fellow, University of New South Wales Faculty of Law; Katherine Lane is a consumer law expert and Vice-Chair of the APF; Nigel Waters is an information practices consultant and former deputy Australian Privacy Commissioner; and Elizabeth Coombs is a researcher at the University of Malta and former NSW Privacy Commissioner.

Executive Summary

The Australian Privacy Foundation (APF) welcomes the contribution made by the ACCC to improving the understanding of how the protection of privacy is central to addressing anti-competitive concerns and consumer protection in the data economy. APF's primary focus in this submission is on the consumer privacy aspects of the Inquiry, but with an eye to the issues of market power, and the trust that is fundamental for public administration in online environments. The APF strongly supports the ACCC's analysis and recommendations, across the board. ACCC's analysis is consistent with a wide range of Australian and international official and private reports over the past three years, demonstrating that there is international recognition of a substantive problem that must be addressed. In particular, APF urges the Government's adoption of the recommendations in Chapter 7 to achieve vital and substantial upgrades in Australia's privacy protection, in order to address the major inroads into privacy because of the enormous growth in data surveillance by the private sector since 2000, the pressing need for a more powerful and much more effective Privacy Commissioner, and to achieve the privacy right of action previously recommended.

For reasons detailed in this Submission (and summarised at its end), APF accordingly expresses its strong support for the adoption by the Australian Government of all of the following Recommendations:

16: Strengthen protections in the Privacy Act
- (a) Update 'personal information' definition
- (b) Strengthen notification requirements
- (c) Strengthen consent requirements and pro-consumer defaults
- (d) Enable the erasure of personal information
- (e) Introduce direct rights of action for individuals
- (f) Higher penalties for breach of the Privacy Act

17: Broader reform of Australian privacy law, having regard to:
1. Objectives
2. Scope
3. Higher standard of protections
4. Inferred information
5. De-identified information
6. Overseas data flows
7. Third-party certification

18: OAIC privacy code for digital platforms, including but not limited to:
1. Information requirements
2. Consent requirements
3. Opt-out controls
4. Children's data
5. Information security
6. Retention period
7. Complaints-handling

19: Statutory tort for serious invasions of privacy

20: Prohibition against unfair contract terms

21: Prohibition against certain unfair trading practices

A submission by the Australian Privacy Foundation to the Australian Government

The Australian Competition and Consumer Commission (ACCC) released the *Final Report* in its *Digital Platforms Inquiry*[2] on 26 July 2019, following a *Preliminary Report* (December 2018). The Australian Government is conducting a public consultation on the ACCC report[3] from 1 August 2019 for twelve weeks,[4] and will announce its response to the report before the end of 2019.

This submission to the Government is by the Australian Privacy Foundation, and is prepared by the below-listed authors with expertise in privacy-related regulation and trust issues. It focuses on the ACCC recommendations that are particularly relevant to privacy issues. It follows an earlier submission on the ACCC draft report.[5] The authors who have contributed to this submission are: Graham Greenleaf, Bruce Arnold, David Lindsay, Roger Clarke, Katherine Lane and Elizabeth Coombs. It is consistent with a range of detailed official and civil society analyses over the past three years.[6]

Fundamental issues: Limiting adverse privacy effects of market dominance

The Australian Privacy Foundation (APF) gives strong support to the ACCC's identification of the market dominance of the Google and Facebook platforms as the underlying core problem which exacerbates or creates the other problems identified in its Report. As ACCC said 'strategic acquisitions by both Google and Facebook have contributed to the market power that they now hold'.[7] We submit that it is essential that the Government give full weight to all of the companies that they 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

---

[2] ACCC Digital Platforms Inquiry <https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry>.

[3] Joint Media Release (Treasurer; Minister for Communications, Cyber Safety and the Arts) Public consultation on the ACCC Digital Platforms Report now open, 1 August 2019 <http://ministers.treasury.gov.au/ministers/josh-frydenberg-2018/media-releases/public-consultation-accc-digital-platforms-report-now>.

[4] Written submissions are due by 12 September 2019, and invited consultation meetings will take place after that: <https://consult.treasury.gov.au/structural-reform-division/digital-platforms-inquiry/>..

[5] 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> .

[6] See for example Canada, House of Commons Committee on Access to Information, Privacy and Ethics (ETHI) and International Grand Committee (May 2019). *Big Data, Privacy & Democracy*; Canada, House of Commons Committee on Access to Information, Privacy and Ethics (ETHI)(2018). *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data-opolies* Ottawa: Government of Canada; Canada, Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia (April 25, 2019). *PIPEDA Report of Findings*; Canada, Elizabeth Denham, Assistant Privacy Commissioner of Canada (July 16, 2009). *Report of the Findings into the Complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act*; European Commission (2019) *Competition Policy for the Digital Era.* Commissioned report by Jacques Crémer, Yves-Alexandre de Montjoye, Heike Schweitzer; France, Facebook Mission (May 2019). *Regulation of social networks – Facebook experiment*. Submitted to the French Secretary of State for Digital Affairs; Germany, Bundeskartellamt (Feb. 6, 2019). *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing (Case Summary)*; Germany, Bundesministerium für Wirtschaft und Energie (2017). *Weißbuch Digitale Plattformen* [White Book Digital Platforms]; OECD (2019). *An Introduction to Online Platforms and Their Role in the Digital Transformation*; United Kingdom, Information Commissioner's Office (Nov. 6, 2018). *Investigation into the use of data analytics in political campaigns: A report to Parliament.*

[7] ACCC draft report, p. 9.

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 ACCC 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'[8]) substantially invented by Google nearly two decades ago, and shortly thereafter 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.[9]

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 (addressed in ACCC Recommendations 1-3);

(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 (addressed in ACCC Recommendations 16-17); 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 (addressed in ACCC Recommendations 8(e)-(g)).

More broadly, failure by Government to effectively address the issues highlighted in this submission 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.

---

[8] 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 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.

[9] 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>

The APF submits that the Government should be conscious of the global and regional dimensions of the issues addressed by the ACCC, which present both challenges and opportunities for effective regulation (eg 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.

ACCC's fundamental Recommendation: Economy-wide privacy reforms

ACCC recommends that almost all its privacy-related recommendations (16(a) – 16(f), and 17, and 19), should be implemented by general amendments to the *Privacy Act 1988* applying to all organisations to which the Act applies, and should not be limited to apply only to digital platforms. It 'considers that economy-wide regulatory reform is needed in some circumstances, and should apply to businesses beyond digital platforms.' ACCC is of the view that the proposed reforms would rarely cause significantly increased compliance costs for businesses not principally involved in commercializing personal data. ACCC's recommended changes to consumer law (Recommendations 20 and 21) are also economy-wide. The only significant sector-specific exception is Recommendation 18, the OAIC Privacy Code for Digital Platforms.

The APF supports very strongly these ACCC recommendations for the economy-wide scope of desirable regulatory reform. The APF regards them as crucial to the effectiveness of the Government's privacy reforms and its broader digital initiatives, including in e-health and digitalisation of government services at the national and state/territory levels. All of these ACCC recommendations, even if they apply with special force to platforms, are equally applicable to all organisations processing personal data, because they would redress general deficiencies to the existing Privacy Act, deficiencies which help make Australia's privacy protections weak and inadequate, and sub-standard compared to those in other countries, and particularly in comparison with the EU GDPR. Reforms based on the ACCC's proposals, and those proposed by the Government in March 2019, therefore present a long-overdue opportunity for a comprehensive reform of Australia's privacy protections.

The additional compliance costs claimed by some businesses opposing economy-wide privacy reforms are unconvincing objections because they over-estimate the costs of compliance and they are outweighed by the benefits of economy-wide privacy protection, especially in terms of increased trust. Further, to define some protections as 'platforms only', would cause confusion and difficulties in application in drawing boundaries around 'platforms', and thus result in increased compliance costs.

Recommendations 1-3 – Measures to address market power of Google and Facebook

APF supports strongly the following ACCC recommendations:

ACCC R1 - Additional privacy-relevant factors in merger laws

- Recommendation 1 (**additional relevant factors in merger laws**, to include the (j) the likelihood that the acquisition would result in the removal from the market of a potential competitor; and (k) the nature and significance of assets, including data and technology, being acquired directly or through the body corporate).

ACCC R2 - Prior notice of acquisitions

- Recommendation 2 (**prior notice of acquisitions**). However, we submit that ACCC Recommendation 2 is not strong enough, because ACCC only recommends that the platforms 'agree to a protocol' without consequences for breaching it. The history of Google and Facebook shows that any voluntary measures are likely to be evaded and defeated (as shown in the FTC's recent enforcement action against Facebook concerning Cambridge Analytica). The only realistic approach when dealing with these companies is legal compulsion coupled with penalties severe enough to be deterrents. The Government should enact at the outset that the platforms are legally compelled to give the required notice, therefore introduce a legal obligation, backed by appropriate penalties, for platforms to give the required notice of acquisitions.

ACCC R4 - Required choices rather than defaults (browsers and search engines)

- Recommendation 3 (required **choices rather than defaults** when operating system providers supply browsers, and when browser providers supply search engines). However, the ACCC recommendation is too narrow, being limited to the current position with Android browsers. APF submits that the Government should enact the ACCC's draft recommendation (not its final version) as a general principle. Such choice in both browsers and search engines is essential to avoiding the concentrated aggregation of user data, and is also consistent with the Privacy By Design & By Default principle now accepted as a key innovation in 3rd generation data privacy laws such as the EU's General Data Protection Regulation (GDPR).

ACCC and data portability

- **Data Portability** – The ACCC Report [2.10.1] says ACCC 'considered whether to recommend specific data portability mechanisms as a means of addressing the market power of digital platforms', but decided not to do so 'at this point in time' despite seeing advantages. However, the ACCC only considered data portability of personal data from a competition perspective, whereas it has already been accepted as a desirable general principle in in 3rd generation data privacy laws such as the EU's General Data Protection Regulation (GDPR). APF submits that the Government should include data portability as part of its economy-wide reforms to the *Privacy Act 1988*, and should not limit it to the Consumer Data Right.

Recommendation 16 – Strengthen protections in the Privacy Act across the economy

The APF submits that the Government should adopt the following ACCC recommendations, although in some cases with clarifications or amendments indicated.

ACCC R16(a) Update 'personal information' definition

> *ACCC recommends 'Update the definition of 'personal information' in the Privacy Act to clarify that it captures technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used identify an individual.'*

APF supports the above recommendation, but notes that special care must be taken to ensure that any definitional changes clearly overcome the difficulties created by the decision of the Federal Court in *Telstra v Privacy Commissioner,*[10]. Such a change would involve making it clear that information is 'about an individual' if it can (given current technologies), contribute to the identification of an individual. Such a clarification of the definition of 'personal information' is important to the ACCC's concerns, because IP addresses, URLs and similar data are among the types of data most commonly correlated by Google, Facebook etc in order to identify data that is about an individual. The GDPR now explicitly includes online identifiers

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

and location data within its definition of 'personal data', and a similar approach is highly desirable in Australia.

APF further 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.

ACCC R16(b) Strengthen notification requirements

> *ACCC recommends 'Require all collection of personal information to be accompanied by a notice from the APP entity collecting the personal information (whether directly from the consumer or indirectly as a third party), unless the consumer already has this information or there is an overriding legal or public interest reason.'*
>
> *ACCC recommends 'The notice must be concise, transparent, intelligible and easily accessible, written in clear and plain language, provided free of charge, and must clearly set out how the APP entity will collect, use and disclose the consumer's personal information. Where the personal information of children is collected, the notice should be written at a level that can be readily understood by the minimum age of the permitted digital platform user.'*
>
> *ACCC recommends 'To provide consumers with a readily understood and meaningful overview of an APP entity's data practices and as a means of reducing their information burden, it may also be appropriate for these requirements to be implemented along with measures such as the use of multi-layered notices or the use of standardised icons or phrases.'*

APF supports these recommendations, but submits that the Government's legislation should be more specific and should specify (as ACCC suggested in its draft Report, p. 227) '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.

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.

ACCC R16(c) Strengthened consent requirements and pro-consumer defaults

> *ACCC recommends 'Require consent to be obtained whenever a consumer's personal information is collected, used or disclosed by an APP entity, unless the personal information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason.'*

> *ACCC recommends 'Valid consent should require a clear affirmative act that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent). This means that any settings for data practices relying on consent must be pre-selected to 'off' and that different purposes of data collection, use or disclosure must not be bundled. Where the personal information of children is collected, consents to collect the personal information of children must be obtained from the child's guardian.'*
>
> *ACCC recommends 'It may also be appropriate for the consent requirements to be implemented along with measures to minimise consent fatigue, such as limiting consent requirements to when personal information is collected for a new purpose, or using standardised icons or phrases to refer to certain categories of consents to facilitate consumers' comprehension and decision-making.'*

APF support these recommendations, but submit that it should specifically state that the onus of proof of compliance with all consent conditions lies with the collector of the information. APF also submit that separate consents should be required for each separate purpose ('unbundling' of bundled consents), and that furthermore, information for which consent is required should be unbundled from any information for which consent is not required. As ACCC states, steps need to also be taken to minimize 'consent fatigue', and particularly to avoid requiring the same consent on multiple occasions.

However APF also 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 informed 'consent' as the legal basis for collecting, using or disclosing any personal information that is not strictly necessary to fulfil the original transaction. 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[11] 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 contends that consent to collection or use or disclosure of any item of personal information can only be 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 made mandatory.

---

[11] 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)

ACCC R16(d) Enable the erasure of personal information

> *ACCC recommends 'Require APP entities to erase the personal information of a consumer without undue delay on receiving a request for erasure from the consumer, unless the retention of information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason.'*

APF supports this recommendation, and gives particular strong support to the fact that the recommendation is not limited in its scope to information provided by the data subject on the grounds of 'consent' in the first place.

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.[12] 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.

The APF has watched with concern that a right to deletion or erasure was dropped from the Consumer Data Right (CDR) legislation (also known as open banking). We understand there is some negotiation to reinstate that right. However, although concern remains that this fundamental right (one that is available in the EU) is not present in recently legislated data portability legislation, its value is not in any way limited to the context of data portability, and it should be explicitly included in reforms based on the ACCC recommendations.

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, and we draw the Government's attention to exploration by the Department of the Treasury about technical mechanisms to facilitate informed consent in relation to the Australian Consumer Data Right.

ACCC R16(e) Introduce direct rights of action for individuals

> *ACCC recommends 'Give individuals a direct right to bring actions and class actions against APP entities in court to seek compensation for an interference with their privacy under the Privacy Act.'*
>
> *'The ACCC recommends that individuals should have a right of action in the Federal Court or the Federal Circuit Court to be able to seek compensatory damages as well as aggravated and exemplary damages (in exceptional circumstances) for the financial and non-financial harm suffered as a result of an infringement of the Privacy Act and the APPs.'*

We give 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

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

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 the ACCC's 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.[13] It would help provide the certainty that business expects in dealing with consumers, governments and other enterprises.

ACCC R16(f) Higher penalties for breach of the Privacy Act

> *ACCC recommends 'Increase the penalties for an interference with privacy under the Privacy Act to mirror the increased penalties for breaches of the Australian Consumer Law.'*

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

[13] 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

Government has already proposed such an increase, noting that the 10% is calculated against local annual turnover.

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. The standard set by the European Union's *General Data Protection Regulation* (GDPR) is 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)). In January 2019 the first administrative fine was made under these provisions, when France's data protection authority (the CNIL) fined Google 50 million euros, and since then the UK Information Commissioner's Office in July 2019 has proposed two fines for large-scale data breaches of £183 million (British Airways) and £99 million (Marriott hotel chain).

This 'EU benchmark' of '2-4%' is being reflected in Bills in the process of enactment in many countries. It has already been enacted in Korea, at the level of 3% of global annual turnover. One fine of US$4.5 million (approximately) has been made against a shopping mall for a data breach. It has been proposed in India.

We submit 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, and the proportion should be in the range 2-4%. 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.

In addition to this proposed penalty proportional to turnover, APF submits that another potent form of deterrent, particularly applicable to data privacy breaches, should be introduced. In South Korea, statutory damages may 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 3 million won (US$3,000) per person to a class of those whose data was leaked. Claimants have no need to prove actual damage. Some US laws have similar provisions. 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. We submit that ACCC should recommend such a statutory damages provision.

Reflecting comments above about the global nature and offshore incorporation of leading platforms we note that the ACCC is not in a position to provide effective deterrence through imprisonment or disqualification of overseas corporate executives. Tangible financial

penalties and formal undertakings not to repeat misbehaviour are therefore salient; they are consistent with the ACCC's compliance pyramid strategy.

Australian Government proposed reforms to the Privacy Act (March 2019)

In March 2019 the Government announced[14] that amendments to the Privacy Act would be made to achieve the following objectives (italicised below). It said 'Legislation will be drafted for consultation in the second half of 2019.' Since these reforms will probably be enacted at the same time as those recommended by the ACCC, APF takes the opportunity to make submissions on these Government proposals as well.

Govt. 1: Increase penalties

> *Increase penalties for all entities covered by the Act, which includes social media and online platforms operating in Australia, from the current maximum penalty of $2.1 million for serious or repeated breaches to $10 million or three times the value of any benefit obtained through the misuse of information or 10 per cent of a company's annual domestic turnover – whichever is the greater.*

This is essentially the same penalty regime, and scope, as ACCC recommendation 16(f). APF supports such a change, but considers that the EU approach of 2-4% of global turnover would be preferable, as discussed above.

Govt. 2: OAIC infringement notice powers

> *Provide the Office of the Australian Information Commissioner (OAIC) with new infringement notice powers backed by new penalties of up to $63,000 for bodies corporate and $12,600 for individuals for failure to cooperate with efforts to resolve minor breaches.*

APF notes that this is a very limited power which only applies to non-cooperation with the OAIC, and is not a penalty that the OAIC can apply for minor breaches of the Act. It would be preferable if the OAIC could impose directly minor penalties for minor breaches, instead of having to take the matter to the Federal Court before a penalty can be imposed (which has never occurred since this reform was made in 2012).

Govt. 3: OAIC 'other options'

> *Expand other options available to the OAIC to ensure breaches are addressed through third-party reviews, and/or publish prominent notices about specific breaches and ensure those directly affected are advised.*

APF supports this proposed change.

Govt. 4: Social media 'deletion' requirement

> *Require social media and online platforms to stop using or disclosing an individual's personal information upon request.*

This proposal is consistent with, but can now be superseded by, ACCC recommendation 16(d), which is preferable.

Govt. 5: Extra protection for vulnerable groups

> *Introduce specific rules to protect the personal information of children and other vulnerable groups.*

---

[14] Attorney-General, Christian Porter and Minister for Communications and the Arts, Mitch Fifield, Media release: 'Tougher penalties to keep Australians safe online' 24 March 2019 <https://www.attorneygeneral.gov.au/Media/Pages/Tougher-penalties-to-keep-australians-safe-online-19.aspx>

APF supports this proposed change in principle, but no details are given except that it will include 'even stronger regimes to address these issues when the user is a child or other vulnerable person' in relation to request to stop using personal information.

Govt. 6: A 'code for social media and online platforms'

The government also proposes legislative amendments:

> *which will result in a code for social media and online platforms which trade in personal information. The code will require these companies to be more transparent about any data sharing and requiring more specific consent of users when they collect, use and disclose personal information.*

This proposal is consistent with, but can now be superseded by, ACCC recommendation 18, which is in much greater detail and is preferable.

Govt. 7: Additional funding to OAIC

The government also proposes that:

> *'The OAIC will be provided with an additional $25 million over three years to give it the resources it needs to investigate and respond to breaches of individuals' privacy and oversee the online privacy rules.'*

APF supports the provision of more resources to the OAIC. The OAIC at present has a six month delay before it even starts to investigate a complaint. However, the provision of 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 recent inclusion in the *Privacy Act* of the s96(1)(c) right of appeal against s52 Determinations by the Commissioner[15] 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.[16] For 2011-14 the average was two per year.[17] Since 2014 the average has risen to 5.5 per year,[18] but this still represents less than one appealable decision every two months. Furthermore, these are something close to 'self-selected' complaints, the ones

---

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

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

[17] 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.

[18] 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'.

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 5 successful complainants out of 5.5 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.

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. 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 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.

Recommendation 17 – Broader reform of Australian privacy law (ACCC proposals)

> *ACCC recommend that broader reform of Australian privacy regime should be considered to ensure it continues to effectively protect consumers' personal information in light of the increasing volume and scope of data collection in the digital economy, and should have regard to the following issues:*

In addition to the ACCC's specific recommendations for reform of the Privacy Act, and the Government's March 2019 proposals for reform, the ACCC also recommends that the Government examine additional reforms (italicised below). APF supports the Government revising the Privacy Act to address all these issues, except to the extent that we comment below on some of them. However, it is important that the other reforms specifically recommended by the ACCC, and the reforms already proposed by the Government should not be delayed while these additional reforms are considered.

ACCC R17.1 Objectives

> ***Objectives:*** *whether the objectives of the Privacy Act should place greater emphasis on privacy protections for consumers including protection against misuse of data and empowering consumers to make informed choices*

ACCC R17.2 Scope and exemptions

> ***Scope**: whether Privacy Act should apply more to some of the entities which are currently exempt (for example, small businesses, employers, registered political parties).*

APF gives very strong support to such broadening of the scope of the Act. Removal of the many unjustifiable exemptions from the Privacy Act, such as those cited by the ACCC, was one of the major recommendations of the Australian Law Reform Commission in its review of the Privacy Act. This is an overdue reform. The Cambridge Analytica/Facebook scandal has demonstrated the potential dangers of exempting political parties from the Act. Lack of transparency in the political uses of personal information increases the risk of voters disengaging from mainstream parties in favour of fringe groups. 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. The so-called 'small business exemption' is a major impediment to Australia obtaining a positive adequacy assessment from the EU, and provisions in Japan's laws with similar effect were removed from its law prior to its adequacy application.

ACCC R17.3 Higher standard of protections

> ***Higher standard of protections:** whether the Privacy Act should set a higher standard of privacy protection, such as by requiring all use and disclosure of personal information to be by fair and lawful means.*

APF supports the extension of the 'fair and lawful means' requirement to all aspects of processing of personal information (not only use and disclosure), whereas at present it only applies to collection of personal information.

ACCC R17.4 Inferred information

> ***Inferred information:** whether the Privacy Act should offer protections for inferred information, particularly where inferred information includes sensitive information, such as information about an individual's health, religious beliefs, or political affiliations.*

APF supports such a change, which should be dealt with as part of the review of the definition of 'personal information' in ACCC recommendation 16(a).

ACCC R17.5 De-identified information

> ***De-identified information:** whether there should be protections or standards for de-identification, anonymisation and pseudonymisation of personal information to address the growing risks of reidentification as datasets are combined and data analytics technologies become more advanced*

APF submits that, at a minimum, Australia's anonymisation provisions should be aligned with those of the European Union's GDPR. This should be dealt with as part of the review of the definition of 'personal information' in ACCC recommendation 16(a). It is fundamentally important to recognise that successive empirical research reports have demonstrated the ease and potential impact of reidentification of supposedly 'deidentified' data, with Australian studies ranging from Victoria's Myki system to very sensitive health data.

ACCC R17.6 Overseas data flows and EU 'adequacy'

> ***Overseas data flows:** whether the Privacy Act should be revised such that it could be considered by the European Commission to offer 'an adequate level of data protection' to facilitate the flow of information to and from overseas jurisdictions such as the EU, and*

APF considers 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), as Japan has done in 2019, New Zealand did in 2013, and Korea is likely to do shortly. 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 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.

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.

ACCC R17.7 Third-party certification

> ***Third-party certification****: whether an independent certification scheme should be introduced.*

APF's submission on the ACCC's draft report stated that such certification schemes must be developed with considerable care to avoid the problems, mentioned below, but APF is not completely opposed, just sceptical, about certification being used as a means of implementing 'demonstrable accountability' (in GDPR terms). This is still APF's position.

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 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 ACCC will need to avoid these dangers in its final proposals. It is proposing to 'require certain businesses' to be certified, which should 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 in the ACCC's proposals is that the certification bodies would be certifying against compliance with the *Privacy Act*. In contrast with the very poor example of the APEC-CBPRs (Cross-border Privacy Rules system), 'Accountability Agents' such as TRUSTe (now TrustArc), only certify against the far lower standard of the APEC Privacy Framework, not against the standard of national laws of the companies certified.[19] This ACCC-proposed certification system should not be confused or combined in any way with the Australian

[19] 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

government's proposal to join the APEC-CBPRs, because of these inconsistent and irreconcilable standards for certification.

Recommendation 18 – OAIC Privacy Code for Digital Platforms

The ACCC considers that 'this recommendation could align with the Government's March 2019 announcement to create a legislated code applying to social media and online platforms which trade in personal information.'

> *An enforceable code of practice be developed by the OAIC, in consultation with industry stakeholders, to enable proactive and targeted regulation of digital platforms' data practices (DP Privacy Code). The code should apply to all digital platforms supplying online search, social media, and content aggregation services to Australian consumers and which meet an objective threshold regarding the collection of Australian consumers' personal information.*

APF submits that the range of stakeholders with whom the code is to be developed must extend well beyond 'industry stakeholders' as that term is commonly and very narrowly interpreted, and must include Civil Society organisations, and independent experts, with expertise and/or interests in the operation of digital platforms, not least including the APF, EFA and ACCAN. As ACCC recommends below, it should also be involved in the development of the code. APF considers ACCC involvement is essential because of the OAIC's very poor track-record in enforcement of the Privacy Act.

> *The DP Privacy Code should be enforced by the OAIC and accompanied by the same penalties as are applicable to an interference with privacy under the Privacy Act. The ACCC should also be involved in developing the DP Privacy Code in its role as the competition and consumer regulator. The DP Privacy Code should contain provisions targeting particular issues arising from data practices of digital platforms, such as:*

APF supports the development of such a code, and that it should be an enforceable code, but only to the extent that its provisions cannot derogate from the protections provided by the terms of the Privacy Act, as interpreted by the courts. Any such derogations should be invalid. The OAIC must not be given any opportunity to reduce statutory provisions. However, courts should be able to consider the code when interpreting provisions in the Act. As the ACCC notes (p. 482), codes made by the OAIC under Part IIIB of the Privacy Act 'may impose additional requirements to those imposed by the APPs, so long as the additional requirements are not contrary to, or inconsistent with, the APPs'. The APF considers that this is preferable to separate legislation to amend the Act to create a code. A Part IIIB code might also allow speedier development while legislation is still being developed.

APF submits that the DP Privacy Code should be enforceable directly in the courts by individuals, in the same way that ACCC recommends that the rest of the Act be so enforceable (ACCC R16(e)).

Submissions by various digital platform representatives that such a code is not needed because they already comply with some elements of it are intended to obfuscate, avoid uniformity, and avoid penalties, and were correctly rejected by the ACCC (p. 483).

Except to the extent noted in the following comments, APF supports the ACCC's following recommendations for content of the code.

ACCC R18.1. Information requirements:

> *1. Information requirements: requirements to provide and maintain multi-layered notices regarding key areas of concern and interest for consumers. The first layer of this notice*

should contain a concise overview followed by more detailed information in subsequent layers provided to consumers. The final layer should contain all relevant information that details how a consumer's data may be collected, used, disclosed and shared by the digital platform, as well as the name and contact details for each third party to whom personal information may be disclosed.

ACCC R18.2. Consent requirements

2. Consent requirements: requirements to provide consumers with specific, opt-in controls for any data collection that is for a purpose other than the purpose of supplying the core consumer-facing service and, where consents relate to the collection of children's personal information, additional requirements to verify that consent is given or authorised by the child's guardian.

APF supports this proposal, particularly because it goes some distance toward the implementation of the 'Privacy by Default' principle, by requiring consumers to opt-in to having their privacy invaded (the 'No Privacy By Design' options usually favoured by the platforms). It also implements the 'unbundling' of consents, which the APF has recommended as a desirable general reform.

APF also supports the ACCC's rejection of bases other than consent for non-core uses of personal data collected by digital platforms, and particularly a 'legitimate interests' basis for collection, which is still ill-defined where it is used in the GDPR (p. 489).

ACCC R18.3. Opt-out controls

3. Opt-out controls: requirements to give consumers the ability to select global opt-outs or optins, such as collecting personal information for online profiling purposes or sharing of personal information with third parties for targeted advertising purposes.

ACCC R18.4. Children's data

4. Children's data: additional restrictions on the collection, use or disclosure of children's personal information for targeted advertising or online profiling purposes and requirements to minimize the collection, use and disclosure of children's personal information.

ACCC R18.5. Information security

5. Information security: requirements to maintain adequate information security management systems in accordance with accepted international standards.

ACCC R18.6. Retention period

6. Retention period: requirements to establish a time period for the retention of any personal information collected or obtained that is not required for providing the core consumer-facing service.

ACCC R18.7. Complaints-handling

7. Complaints-handling: requirements to establish effective and timely mechanisms to address consumer complaints.

Recommendation 19 – Statutory tort for serious invasions of privacy

Introduce a statutory cause of action for serious invasions of privacy, as recommended by the Australian Law Reform Commission (ALRC). This cause of action provides protection for individuals against serious invasions of privacy that may not be captured within the scope of the Privacy Act. The cause of action should require privacy to be balanced against other public interests, such as freedom of expression and freedom of the media. This

> *statutory cause of action will increase the accountability of businesses for their data practices and give consumers greater control over their personal information.*

APF gives strong endorsement to Recommendation 19. 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.[20]

The Australian Privacy Foundation made submissions[21] to the ALRC during its enquiry which were stronger at various points than the ALRC's final recommendations. A NSW Parliamentary Committee also recommended in 2016 a statutory cause of action[22] 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. The Foundation 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 argues that the impact on freedom of speech, and on media operations, will be minimal (pp. 494-5).

For reasons well-explained by the ACCC (p. 496), the proposed right of individual direct enforcement of the Privacy Act (ACCC R16(e)) is a necessary complement to the statutory action for serious invasions of privacy. APF gives strong support to both reforms being enacted.

ACCC economy-wide consumer law recommendations affecting privacy

ACCC makes two recommendations involving amendments to the Competition and Consumer Act 2010 which, if adopted, will have a very significant effect on the protection of privacy in relation to digital platforms, and to other categories of businesses adversely affecting privacy. These reforms will also bring consumer protection regulators into central roles in the protection of privacy in Australia, taking the sole responsibility for this out of the hands of the OAIC. APF supports both recommendations, and regards them as central to the ACCC reform agenda.

Recommendation 20 – Prohibition against Unfair Contract Terms

> *Amend the Competition and Consumer Act 2010 so that unfair contract terms are prohibited (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.*

---

[20] 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.

[21] 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

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

The ACCC has concluded that the current unfair contract terms (UCT) provisions do not provide sufficient deterrence. 'This recommendation would allow the ACCC to hold businesses (including digital platforms) to account for including UCTs, not just to have UCTs declared void (as is currently the case).' Furthermore, it says '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 digital platforms and consumers over any potential UCTs that digital platforms may wish to use in their terms of use and privacy policies' (p. 497). This is therefore an economy-wide recommendation.

This recommendation is therefore a fundamental aspect of the ACCC's proposals for privacy regulation of platforms, and one to which the APF gives strong support.

Recommendation 21 – Prohibition against certain unfair trading practices

> *Amend the Competition and Consumer Act 2010 to include a prohibition on certain unfair trading practices. The scope of such a prohibition should be carefully developed such that it is sufficiently defined and targeted, with appropriate legal safeguards and guidance.*

ACCC considers that an 'unfair practices' prohibition' would be appropriate to address conduct not currently caught by the consumer protection laws but which has the potential for significant consumer harm'. It would go beyond the scope of the misleading or deceptive conduct provisions on which Australian consumer law is largely based. Because 'the practices of concern identified during the Inquiry are not confined to digital platforms', it proposes economy-wide reforms. Such a prohibition is currently being considered by consumer affairs authorities in all Australasian jurisdictions, and it is through this forum that ACCC intends to pursue its recommendation.

ACCC identifies the privacy-related reasons for these reforms: 'consumer transactions with digital platforms often feature acute information asymmetries and bargaining power imbalances and the existing regulatory framework does not effectively deter data practices that exploit these characteristics' (p. 499). The examples identified by ACCC which could fall under this provision (of which more details are given – see p. 498) include:

- "businesses collecting and/or disclosing consumer data without express informed consent
- businesses failing to comply with reasonable data security standards, including failing to put in place appropriate security measures to protect consumer data
- businesses unilaterally changing 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
- businesses 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
- business 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."

This list of examples, its clear relevance to key privacy-abusing practices of digital platforms, and its further relevance to other privacy-abusing businesses, makes it clear that this reform would add a new form of analysis and regulatory action to Australian privacy regulation, complementary to the analysis and action of the ACCC.

As ACCC points out, overseas consumer protection authorities (including in the EU, UK, USA, Canada and Singapore) has some form of unfair practices authority. In particular "In the US, the FTC [Federal Trade Commission] views that its 'unfairness authority' under the FTC Act, along with its 'deception authority' (similar to the ACL's misleading or deceptive conduct provisions) provide a complementary set of provisions that allow it to address the types of harm that are not otherwise captured by a standalone 'deception authority'." Adopting such an approach would therefore align Australian law with the principal current form of privacy protection in the USA. APF considers this would be very valuable, enabling Australian regulators to benefit from American experience, and from equivalent experience in other jurisdictions, in regulating what will often be the same online platforms.

Summary of submissions made by APF

The Australian Privacy Foundation's submissions to the Government concerning the ACCC Final Report may be summarised in the following propositions:

ACCC's fundamental Recommendation: Economy-wide privacy reforms – APF supports very strongly ACCC recommendations for the economy-wide scope of desirable regulatory reform (recommendations (16(a) – 16(f), and 17, and 19)).

Recommendations 1-3 – Measures to address market power of Google and Facebook – APF supports strongly the following ACCC recommendations:

- Recommendations 1 (**additional relevant factors in merger laws);**
- Recommendation 2 (**prior notice of acquisitions**), but APF submits it is not strong enough, and that the Government should enact at the outset that the platforms are legally compelled to give the required notice.
- Recommendation 3 (required **choices rather than defaults** when operating system providers supply browsers, and when browser providers supply search engines), but APF submits the ACCC recommendation is too narrow, and that the Government should enact the ACCC's draft recommendation (not its final version) as a general principle.

Data Portability – APF submits that the Government should include data portability as part of its economy-wide reforms to the *Privacy Act 1988*, and should not limit it to the Consumer Data Right.

Recommendation 16 – Strengthen protections in the Privacy Act across the economy – The APF submits that the Government should adopt the following ACCC recommendations, although in some cases with clarifications or amendments indicated:

- **ACCC R16(a) Update 'personal information' definition –** APF submits that special care must be taken to ensure that any definitional changes clearly overcome the difficulties created by the decision of the Federal Court in *Telstra v Privacy Commissioner.* APF further 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.

- **ACCC R16(b) Strengthen notification requirements – APF** submits that the Government's legislation should be more specific and should specify details as ACCC suggested in its draft Report.
- **ACCC R16(c) Strengthened consent requirements and pro-consumer defaults –** APF submit that this recommendation should specifically state that the onus of proof of compliance with all consent conditions lies with the collector of the information; that separate consents should be required for each separate purpose ('unbundling' of bundled consents); and that information for which consent is required should be unbundled from any information for which consent is not required; that the 'related secondary purpose within reasonable expectations' test must also be tightened; and that the "take it or leave it" approach to consent should be clearly interpreted as an unfair term.
- **ACCC R16(d) Enable the erasure of personal information –** APF submits that any erasure rights should explicitly include a 'de-linking' right (sometimes called the 'right to be forgotten').
- **ACCC R16(e) Introduce direct rights of action for individuals –** APF gives strong support to this Recommendation, 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.
- **ACCC R16(f) Higher penalties for breach of the Privacy Act –** APF submits that the preferable standard 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.
- 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 Korean, 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.

Australian Government proposed reforms to the Privacy Act (March 2019) – APF gives general support to the Australian government reforms to the Privacy Act proposed in March 2019.

Recommendation 17 – Broader reform of Australian privacy law (ACCC proposals) – APF supports the Government revising the Privacy Act to address all the issues where the ACCC recommends that broader reforms of the Privacy Act should be considered, except to the extent that we comment on some of them.

Recommendation 18 – OAIC Privacy Code for Digital Platforms – APF submits that:

- the stakeholders' with whom the code is to be developed must extend well beyond 'industry stakeholders' as that term is commonly and very narrowly interpreted;
- that ACCC involvement is essential because of the OAIC's very poor track-record in enforcement of the Privacy Act;
- that it should be an enforceable code, but only to the extent that its provisions cannot derogate from the protections provided by the terms of the Privacy Act, as interpreted by the courts;

- that the code should be enforceable directly in the courts by individuals, in the same way that ACCC recommends that the rest of the Act be so enforceable;
- the ACCC's recommendations for the content of the code should be followed.

ACCC economy-wide consumer law recommendations affecting privacy – APF supports both ACCC consumer law recommendations, and regards them as central to its reforms:

- Recommendation 20 – Prohibition against Unfair Contract Terms
- Recommendation 21 – Prohibition against certain unfair trading practices