Digital platforms: The need to restrict surveillance capitalism

Australian Privacy Foundation submission to the ACCC

Digital Platforms Inquiry—preliminary report

Graham Greenleaf, Anna Johnston, Bruce Arnold, David Lindsay, Roger Clarke & Elizabeth Coombs[1] – on behalf of the Australian Privacy Foundation
22 February 2019

A submission by the Australian Privacy Foundation

[The ACCC *Preliminary Report* (December 2018) on its Digital Platforms Inquiry is at https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry.] This submission by the Australian Privacy Foundation, and prepared by the below-listed authors with expertise in privacy-related issues, focuses on the ACCC recommendations that are particularly relevant to privacy issues. The authors who have contributed to this submission are: Graham Greenleaf, Anna Johnston, Bruce Arnold, David Lindsay, Roger Clarke and Elizabeth Coombs.

The fundamental issue: Limiting the adverse effects of surveillance capitalism

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 draft Report. As ACCC says

[1] Graham Greenleaf AM is Professor of Law & Information Systems at the University of New South Wales; Anna Johnston is Principal of Salinger Privacy and a former Deputy NSW Privacy Commissioner; Dry 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 Adjunct Professor, University of New South Wales Faculty of Law; and Elizabeth Coombs is a researcher at the University of Malta and former NSW Privacy Commissioner.

'strategic acquisitions by both Google and Facebook have contributed to the market power that they now hold' (p.9). We submit that it is essential that the ACCC 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 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 'surveillance capitalism', [2] or 'the surveillance economy', substantially invented by Google nearly two decades ago, and shortly thereafter adopted by Facebook, which are still its dominant exponents. They are the dominant 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 very relevant recent developments, German regulators have ordered Facebook to restrict data collection, by requiring that user consent be obtained before combining WhatsApp, Instagram, and Facebook account data.[3]

There are three aspects of surveillance capitalism that are of particular relevance to the ACCC's enquiry: (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 Recommendations 1-3); and (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 Recommendations 8-10); and (iii) the global operation of leading digital platforms, providing the salient corporations with both sufficient revenue to disregard small scale penalties and an imperative to engage in regulatory arbitrage, in particular resisting effective regulation in a jurisdiction such as Australia on the basis that an effective regime will influence policymakers in existing or emerging markets (addressed in Recommendations 8(e)-(g)).

The APF considers that the ACCC should be conscious of that global and regional dimension, which presents both challenges and opportunities for effective regulation (eg consistency

[2] 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.

[3] 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>

with practice in the European Union and recognition that corporations such as Facebook have consistently demonstrated a willingness to evade responsibility by disingenuously claiming that they operate outside EU law). In construing effective regulation the ACCC should be conscious that digital platforms are susceptible to misuse for 'fake news' (including inappropriate political communication and data gathering, whether direct 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. The ACCC is significant given the perceived incapacity of other regulators such as the Therapeutic Goods Administration and the OAIC, in particular because of their lack of transparent and timely responses (which we discuss below).

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

We support strongly Recommendations 1 (additional relevant factors in merger laws, to include the amount and nature of data acquired in a merger), Recommendation 2 (prior notice of acquisitions), and Recommendation 3 (required choices rather than defaults when operating system providers supply browsers, and when browser providers supply search engines).

We submit that Recommendation 2 is not strong enough, because the history of Google and Facebook shows that any voluntary measures will be evaded and defeated, and that the only realistic approach when dealing with these companies is legal compulsion coupled with penalties severe enough to be deterrents. The ACCC should state that platforms will be legally compelled to give the required notice.

Recommendation 8—use and collection of personal information

ACCC R8: The ACCC proposes to recommend the following amendments to the Privacy Act to better enable consumers to make informed decisions in relation to, and have greater control over, privacy and the collection of personal information.

We support the ACCC's approach of reforming those parts of the *Privacy Act 1988* which are most relevant to the ACCC's enquiry, rather than another wholesale attempt to reform the *Privacy Act*. However, we submit that there are some additional specific aspects of the *Privacy Act* that should come within the ACCC's reform agenda because of their relevance to ACCC's objectives and proposals.

R 8(a)-(b): 'reducing information asymmetries to improve the transparency of digital platforms' data practices'

ACCC R 8(a) ***Strengthen notification requirements:*** *Introduce an express requirement that the collection of consumers' personal information directly or by a third party is accompanied by a notification of this collection that is concise, transparent, intelligible and easily accessible, written in clear and plain language (particularly if addressed to a child), and provided free of charge.*

We support this recommendation, but submit that it should be more specific and should specify (as ACCC suggests) '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' (p. 227). 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).

While we support this recommendation, we submit that it will not be sufficient to achieve its aims unless the definition of 'personal information' in the *Privacy Act* is amended to clarify that it does include an IP address, a URL, or other information which can be used to identify an individual, thus clarifying the effect of the decision of the Federal Court in *Telstra v Privacy*

Commissioner.[4] 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 and location data within its definition of 'personal data', and a similar approach is highly desirable in Australia.

We further submit that the definition of 'personal information' in the *Privacy Act* ought 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 the individual cannot be *identified* per se from the data.

ACCC R 8(b) ***Introduce an independent third-party certification scheme:*** *Require certain businesses, which meet identified objective thresholds regarding the collection of Australian consumers' personal information, to undergo external audits to monitor and publicly demonstrate compliance with these privacy regulations, through the use of a privacy seal or mark. The parties carrying out such audits would first be certified by the OAIC.*

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. Theses 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.[5] This ACCC-proposed certification system should not be confused or combined in any way with the Australian government's proposal to join the APEC-CBPRs, because of these inconsistent and irreconcilable standards for certification.

Our submission therefore is that such certification schemes must be developed with considerable care to avoid the above problems, but we are not completely opposed, just

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

[5] 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

sceptical, about certification being used as a means of implementing 'demonstrable accountability' (in GDPR terms).

R 8 (c)- d): 'provide consumers with stronger mandated controls over the collection, use, disclosure and erasure of their personal information to lessen the bargaining power imbalance between consumers and digital platforms.'

ACCC R 8(c) ***Strengthen consent requirements:*** *Amend the definition of consent to require express, opt-in consent and incorporate requirements into the Australian Privacy Principles that consent must be adequately informed (including about the consequences of providing consent), voluntarily given, current and specific. This means that settings that enable data collection must be pre-selected to 'off'. The consent must also be given by an individual or an individual's guardian who has the capacity to understand and communicate their consent.*

We support this recommendation, 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.

ACCC notes that 'It may also be appropriate to review the instances where consent is required under the APPs to ensure that each instance of data collection is accompanied by a specified primary or secondary purpose and that separate consents are obtained for use and for disclosure' (p. 229). We submit that such 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.

However we also submit 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 '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 of a welfare recipient's personal information by Centrelink to the media[6], demonstrates the inability of APP 6.2 to constrain even egregious behaviours.

ACCC R 8(d) ***Enable the erasure of personal information:*** *Enable consumers to require erasure of their personal information where they have withdrawn their consent and the personal information is no longer necessary to provide the consumer with a service.*

We support this recommendation, but submit that it is far too limited in its scope, being restricted to information provided by the data subject on the grounds of 'consent' in the first place. 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.[7] In both pre- and post-GDPR, the right to 'de-linking', 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. We

[6] See https://www.oaic.gov.au/media-and-speeches/statements/centrelink-debt-recovery-system#concluding-statement-centrelink-release-of-personal-information

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

submit 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, the ACCC needs to consider whether its recommendation should be reworded so as to expressly incorporate a de-linking right such as adopted by courts in the EU.

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

R 8 (e)-(g): 'increase the deterrence effect of the Privacy Act'

The ACCC's is correct in identifying the the lack of any deterrent effect of the *Privacy Act 1988*, i to any privacy breaches by companies, particularly those of the scale and financial resources of Google or Facebook, but also of most smaller companies. However, ACCC also needs to recognise that these deficiencies are exacerbated by the current and past administration of the Privacy Act, as discussed in the following.

8(e) ***Increase the penalties for breach:*** *Increase penalties for breaches of the Privacy Act to at least mirror the increased penalties for breaches of the Australian Consumer Law.*

While any increase in penalties for breaches of the Privacy Act would be an improvement on the current situation, we do 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.

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.

We submit that if Australian privacy law is to have a deterrent effect on 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, we submit that another potent form of deterrent, particularly applicable to data privacy breaches, should be introduced. In 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.

ACCC R 8(f) ***Introduce direct rights of action for individuals****: Give individual consumers a direct right to bring actions for breach of their privacy under the Privacy Act.*

We give strong support to this Recommendation. The investigation and enforcement functions of the Privacy Commissioner have operated in a very unsatisfactory manner for many reasons, only some of which can be addressed by providing more resources to the OAIC.

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 Foundation 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* (Cth) is that agency's ongoing emphasis on closed-door consultation 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 desire across both industry and civil society for information that will enable stakeholders to understand how the OAIC is interpreting the Privacy Act. Litigation provides 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.[8]

[8] 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

ACCC R 8(g) ***Expand resourcing for the OAIC to support further enforcement activities:*** *Provide increased resources to equip the OAIC to deal with increasing volume, significance, and complexity of privacy-related complaints.*

The OAIC at present has a six month delay before it even starts to investigate a complaint. We support the provision of more resources to the OAIC.

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, there are only a handful of non-trivial cases that 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[9] 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.[10] For 2011-14 the average was two per year.[11] Since 2014 the average has risen to 5.5 per year,[12] but this still represents less than one appealable decision every two months. 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 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.

---

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

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

[11] 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.

[12] 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'.

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.

We therefore submit that the ACCC should recommend the removal of the s41(1)(a) and s41(2)(a) impediment 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 9—OAIC Code of Practice for digital platforms

ACCC R 9: The ACCC proposes to recommend that the OAIC engage with key digital platforms operating in Australia to develop an enforceable code of practice under Part IIIB of the Privacy Act to provide Australians with greater transparency and control over how their personal information is collected, used and disclosed by digital platforms. A code would allow for proactive and targeted regulation of digital platforms' data collection practices under the existing provisions of the Privacy Act.

The code of practice would likely contain specific obligations on how digital platforms must inform consumers and how to obtain consumers' informed consent, as well as appropriate consumer controls over digital platforms' data practices. The ACCC should also be involved in the process for developing this code in its role as the competition and consumer regulator.

We support this recommendation, and in particular the involvement of the ACCC in the development of such a Code of Practice. The ACCC's report has demonstrated the unique role that digital platform operators play, and studies of surveillance capitalism/economy reinforce this by demonstrating how their role in driving the mechanisms of surveillance capitalism is distinctively different and more important than those of the purchasers of the surveillance services they provide. The ACCC's report also demonstrates that the societal dangers of digital platform operators go well beyond issues of privacy (and therefore beyond the competence of the OAIC), and require broader understandings of competition and discrimination issues that the ACCC is better equipped to provide.

For such a Code to address the key issues effectively requires comprehensive consultation before, during and after development of a draft Code, in order to identify emerging issues. At present, these might include matters such as AI/automated processing and gender impacts including processes for take-downs.

Recommendation 10—serious invasions of privacy

ACCC R 10: The ACCC proposes to recommend that the Government adopt the Australian Law Reform Commission's recommendation to introduce a statutory cause of action for serious invasions of privacy to increase the accountability of businesses for their data practices and give consumers greater control over their personal information.

We endorse strongly Recommendation 10. The ALRC's examination of this issue was very thorough and its recommendations well-balanced.

The Australian Privacy Foundation made submissions[13] 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[14] which went further than the ALRC recommendations, which were confined to intentional or reckless elements, 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 ACCC may wish to examine both the APF submission and the NSW report, and to consider strengthening its recommendation accordingly. The Foundation notes that there have been a succession of other reports recommending establishment of a statutory cause of action. Such development is consistent with the implied freedom of political communication and would not impermissibly encumber the operation of established or emerging media organisations. The Foundation cautions against claims by stakeholders whose systemic disregard of privacy and willingness to endorse criminal activity, such as hacking, by agents has resulted in condemnation by courts and in settlements that in the United Kingdom are reported to amount to over 100 million pounds. In essence, advocacy by commercial entities that are proven to not regulate themselves should not be accepted on face value.

Proposed areas for further analysis and assessment

The preliminary report identifies 9 areas which require further analysis and assessment. In this submission, we address two of those areas which are particularly relevant to privacy protection: deletion of user data and opt-in targeted advertising.

The preliminary report indicates that the ACCC is considering the possibility of an explicit obligation on platform operators to delete all user data once a user ceases to use the platform's services or after a set period. Given the value of user data for platforms, the retention of data beyond what is necessary for the purposes of the user effectively represents a windfall for platform operators, explaining the difficulties often facing users seeking to remove their data from social media platforms. Moreover, the more data that is held about users the more risks there are to user privacy. In order to redress the power imbalance between platforms and users, this submission supports the introduction of an obligation for platform operators, and especially social media platforms, to automatically delete user data (which may include data other than 'personal information') once it is no longer necessary for the purposes of the user.

The preliminary report also indicates that the ACCC is considering introducing an opt-in requirement for the use of targeted advertising by platform providers. As the preliminary report explains, this would not affect the use of advertising by platforms, but would simply require express consent for targeted advertising based on user data. At present, the substantial market power possessed by some platforms means that users have no effective choice but to agree to (or tolerate) the use of their data to generate targeted advertising. The introduction of an opt-in regime for targeted advertising would be an effective mechanism to redress the power imbalance between platform operators and users, while ensuring that those users that may genuinely wish to receive targeted advertising retain this possibility. The APF agrees with the preliminary report that the opt-in requirement for targeted advertising should be applied to all entities that collect user data for this purpose.

[13] 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

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

Summary of submissions made

The Foundation's submissions to the ACCC may be summarised in the eighteen following propositions:

(i) We submit that it is essential that the ACCC give full weight to all of the companies that Google and Facebook 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.

(ii) The issues at stake also go beyond questions of correcting market imperfections. We submit that the ACCC should explicitly recognise that they constitute a new and dangerous economic formation, where flows of data have been used to create what is now widely described as 'surveillance capitalism', or 'the surveillance economy',

(iii) We support strongly Recommendations 1 (additional relevant factors in merger laws, to include the amount and nature of data acquired in a merger), Recommendation 2 (prior notice of acquisitions), and Recommendation 3 (required choices rather than defaults when operating system providers supply browsers, and when browser providers supply search engines).

(iv) We submit that Recommendation 2 is not strong enough, because the history of the platforms shows that any voluntary measures will be evaded and defeated, and that the only realistic approach when dealing with these companies is legal compulsion coupled with penalties severe enough to be deterrents. The ACCC should state that platforms will be legally compelled to give the required notice.

(v) We support Recommendation 8(a), but submit that it should be more specific and should specify (as ACCC suggests) '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'

(vi) We submit that Recommendation 8(a) will not be sufficient to achieve its aims unless the definition of 'personal information' in the *Privacy Act* is amended to clarify that it does include an IP address, a URL, or other information which can be used to identify an individual.

(vii) We further submit that the definition of 'personal information' in the *Privacy Act* ought 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 and thus can be subjected to targeting or intervention, even if the individual cannot be *identified* per se from the data.

(viii) We submit that the certification schemes proposed in Recommendation 8(b) must be developed with considerable care to avoid problems identified in the submission, but do not oppose appropriate certification being used as a means of implementing 'demonstrable accountability'.

(ix) We support Recommendation 8(c) concerning consent, 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; that such separate consents should be required for each separate purpose; and that information for which consent is required should be unbundled from any information for which consent is not required.

(x) We further submit that the ACCC should require companies to rely on 'consent' as the legal basis for collecting, using or disclosing any personal information that is not strictly necessary to fulfil the original transaction.

(xi) We support Recommendation 8(d) to enable the erasure of personal information, but submit that it is far too limited in its scope, being restricted to information

provided by the data subject on the grounds of 'consent' in the first place. We submit that it should be expanded to encompass an Australian equivalent of the EU's 'right to be forgotten'.

(xii) In relation to Recommendation 8(e) concerning increase in the penalties for breach, we submit that if Australian privacy law is to have a deterrent effect on 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%.

(xiii) We further submit that ACCC should in addition recommend a statutory damages provision whereby a specified amount of 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), without need for proof of actual damage by the data subject whose personal data was disclosed.

(xiv) We give strong support to Recommendation 8(f) to introduce direct rights of action for individuals to take actions for breach of the Privacy Act before the Courts, without need to first complain to the OAIC.

(xv) While not opposing Recommendation 8(g) to expand resourcing for the OAIC, we submit this is not the most significant cause of the lack of interpretation of the Privacy Act by courts or tribunals. We submit that the ACCC should recommend the removal of the s41(1)(a) and s41(2)(a) Privacy Act impediment 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.

(xvi) We support Recommendation 9, and in particular the involvement of the ACCC in the development of such a Code of Practice.

(xvii) We endorse strongly Recommendation 10 that there should be a statutory cause of action for serious invasions of privacy. The ALRC's examination of this issue was very thorough and its recommendations well-balanced, but we further submit that the ACCC may also wish to examine both the APF submission to the ALRC and the NSW Parliamentary Committee report on this topic, and to consider strengthening its recommendation accordingly.

(xviii) The ACCC preliminary report identifies 9 areas which require further analysis and assessment, and we submit that two of those areas are particularly relevant to privacy protection and do require such further consideration: deletion of user data and opt-in targeted advertising.

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/