Reset.
AUSTRALIA

Policy Submission

Submission on the Review of the Privacy Act 1988

To: *Attorney-General's Department*
From: *Reset Australia*

Reset Australia would like to thank the Attorney-General's Department for the opportunity to input on the Review of the Privacy Act 1988.

Reset Australia is an independent, non-partisan organisation committed to driving public policy advocacy, research, and civic engagement agendas to strengthen our democracy within the context of technology. We are the Australian affiliate of Reset, the global initiative working to counter digital threats to democracy. As the Australian partner in Reset's international network, we bring a diversity of new ideas home and provide Australian thought-leaders access to a global stage.

We look forward to working with the Attorney-General's Department through this consultation and beyond, as we push this conversation forward to ensure appropriate and considered legislation that protects Australian institutions, citizens and democracy.

Prepared by:
Matt Nguyen
Policy Lead, Reset Australia
matt@au.reset.tech

1.0 Context

Australians' privacy, particularly in relation to personal data, has never been so important. Today's digital platforms have built a system of unfettered and limitless personal data collection that has resulted in the most profitable products of the 21st century.

By building comprehensive profiles of their users that encapsulate their interests, vices, political leanings, triggers and vulnerabilities, they are able to predict our engagement behaviour, using their algorithms to constantly calculate what content has the greatest potential for keeping us engaged and serving this to us. Their business models are geared towards the single objective of keeping us on their products, to maximise their opportunity to generate advertising revenue.

The algorithms built by these companies already dictate all of the content and information we consume. The use of services provided by the major digital platforms have become ubiquitous to the Australian way of life. With over 85% of Australians using social media 'most days',[1] the role that the digital platforms such as Facebook (Instagram, WhatsApp, Facebook), Twitter, Snapchat, TikTok and Google (YouTube and Google) play in our society has become fundamental to how we live, work and entertain ourselves. Slowly, but at an increasing rate, we are starting to experience the spectrum of harms that have arisen from this relationship. From the acceleration in the breakdown of public trust in institutions, democracy and civic debate evidenced through the 2016 US Presidential Election and Brexit, to the public health risks associated with Covid-19 and anti-vaccination disinformation, evidence suggests that content that lean towards the extreme and sensational, is more likely to have higher engagement[2,3] and thus algorithmically amplified.

This has resulted in the explosion of a data economy that has been facilitated through the commoditisation of personal information. This model, termed 'surveillance capitalism' by Shoshanna Zuboff,[4] is predicated on the extraction and exploitation of personal data for the primary purpose of predicting and changing individual behaviour. This emerging model (spearheaded by Google and later Facebook) sets a dangerous precedent for adoption by other industries, and flies against Australian ideals of autonomy, public safety and privacy.

In order to address these emerging harms we must ensure that our concepts of privacy are updated to reflect this changing landscape, in particular our understanding and protection of personal data. Whilst we recognise that this issue sits within a much wider and complex socio-political landscape, we want to impress that at no other point in history have such a small pool of actors had access or the ability to utilise this amount of information with no oversight. The balance between undue regulatory burden and the impacts of privacy degradation, in our opinion has tipped.

---

[1] Yellow Social Media Report (2020) Part One: Consumers. Found at: https://2k5zke3drtv7fuwec1mzuxgv-wpengine.netdna-ssl.com/wp-content/uploads/2020/07/Yellow_Social_Media_Report_2020_Consumer.pdf

[2] Vosoughi et al. (2018), 'The spread of true and false news online', *Science,* found at https://science.sciencemag.org/content/359/6380/1146

[3] Nicas (2 Feb 2018), 'How YouTube Drives People to the Internet's Darkest Corners', *Wall Street Journal* found at https://www.wsj.com/articles/how-youtube-drives-viewers-to-the-internets-darkest-corners-1518020478

[4] Zuboff S (2019), 'The Age of Surveillance Capitalism,' Profile Books, London

Personal information is the bedrock of this phenomenon, and it's time for us as an Australian and global society to ensure that the necessary guidelines are established to protect public interest.

2.0 Response to Issues Paper

2.1 Scope and Application of the Privacy Act

Definition of Personal Information

The current definition of 'personal information' under the Privacy Act 1988 must be updated to account for the data-driven digital environment that we currently exist in, and that is vastly different from the time of the writing of the Act. Under the current definition, 'personal information' is defined as '*information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable'*.[5] This has caused considerable ambiguity in its interpretation, and seeing as this dictates how information is handled under the Australian Privacy Principles (APP), greater clarity must be had in this definition.

Whilst we respect the decision made in *Privacy Commissioner vs Telstra Corporation Ltd. (2017)*[6] by the Australian Federal Court, it has created a major limitation to future-proof our definitions of personal information. The decision to uphold the Administrative Appeals Tribunal lacks a sophistication in understanding that what data might be 'for' isn't mutually exclusive to what the data is 'about'. This is especially true as our governance, communications, economic and social systems are driven more and more by big-data analytics using larger and larger sets of data, continuing to blur these lines to a greater degree. Additionally, this decision leaves open the possibility that metadata could sometimes be considered personal information but provides no clear guidance around these conditions.

It is clear that these definitions must be updated and aligned with international standards in order for us to have proper recognition of the realities of a digital age. The adoption (or alignment to similar effect) of the European Union's (EU) General Data Protection Regulation's (GDPR) definition of personal data should be considered, in particular the definition of 'any information relating to an identified or identifiable natural person'.[7] Building on this, the Privacy Act needs to be updated to include that technical data related to an individual also be considered as 'personal information'. We stress that there are a range of online identifiers that make up technical data, which may include:

- IP addresses,
- metadata,
- RFID tags,
- URLs,
- Geolocation and tracking data
- advertising identifiers,

[5] *Privacy Act 1988* (Cth) pt II div 1
[6] *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4.
[7] Regulation (EU) 2016/679 2016, Article 4

- security and fraud detection identifiers

And that these should be stipulated as personal data to ensure appropriate legal and regulatory recognition of the suite of online data collection instruments often working in concert to identify users on these platforms. This alignment will also decrease the regulatory and compliance burden that many companies operating internationally (specifically within the EU) already face.

Recommendation: Change the current definition of personal information to align more with the EU GDPR's definition of 'personal data' and specifically include technical data and online identifiers within the scope of this definition.

Exemptions

Small Business Exemption

Whilst we understand and support the intention behind the initial inclusion of the small business exemption, modern day challenges and risks small businesses face regarding data protection and privacy illustrate the inadequacy for this exemption to fulfil its desired outcomes.

Efforts must be made to foster and drive innovation in Australia, and as such, we strongly support the exemption's aims of reducing compliance burdens and costs on small businesses. However, new industries born by the start up revolution from e-commerce to 'Software as a Service' (SaaS) have revealed how data collection and analytics are a fundamental part of many business operations.

We strongly agree with the Senate Legal and Constitutional References Committee's recommendation to remove the small business exemption.[8] Whilst we recognise the reasons behind the Government's rejection of this recommendation in 2005, 15 years of technological progress require a complete re-contextualisation of this assessment. In addition to providing a harmonised guidance for regulatory obligations, the removal of this exemption would align us with international standards on privacy requirements for small businesses. This is an especially important step to becoming GDPR compliant, with the failure to do so representing the potential loss of trade and collaboration opportunities with the EU market.

The removal of this exemption must be coupled with increased efforts to support small businesses to achieve their privacy obligations. This may take the form of allocating specific funding for start ups and other small businesses to achieve adequate privacy frameworks and the development and delivery of education materials and programming. Whilst there will be an undeniable compliance cost, efforts must be made to impress upon existing and potential small business owners on the importance and gravity of data protection.

Recommendation: Remove the Small Business Exemption

[8] Senate Legal and Constitutional References Committee, Parliament of Australia, *The Real Big Brother: Inquiry into the Privacy Act 1988* (Report, June 2005) 157

Employee Records Exemption

In keeping with a comprehensive and harmonised approach to privacy obligations, we strongly believe that the employee records exemption must be removed. The right to privacy and the protections afforded under the Act must be extended to employees, with the current provision inadequate to react to modern workplace demands.

As our hunger for data analytics begins to blur the lines between work and personal life, employers have increasingly employed greater forms of data collection and surveillance on their employees. Cases of biometric data collection, social media monitoring, personality and aptitude testing and diversity metric collection illustrate the spectrum of types of personal information collected.

Recommendation: Remove the Employee Record Exemption

Political Exemption

In light of the Cambridge Analytica scandal, all efforts must be made to ensure that adequate protections of personal data be made. The potential for harm that privacy breaches and manipulative surveillance and influence operations within our political system have taken on unprecedented dimensions in the 21st century.

Public and expert support for the removal of this exemption have had a long history, with repeated calls for better protections from minor party leaders, Privacy Commissioners, academics, civil society and the general public.[9] Whilst the stagnant adoption of these reforms can be attributed to domestic partisan vested interests, the real and magnified risks we face in the age of surveillance capitalism must be incorporated into decision-making around this issue.

Malicious actors, both state and non-state, with significant cyber capabilities are exploiting these weaknesses to interfere in our democractic processes. Exemplified by a major cyber-attack in February 2019 which gained access to Liberal, Labor and National party networks just months before a Federal Election,[10] the reality of these harms represent a fundamental risk to our existence as a liberal democracy. The scale and scope of these operations is unprecedented, and has invalidated the original rationale for this exemption. Whilst these issues won't be solved by removing this exemption, the protections afforded by complying with the Privacy Act represent a significant first step to safeguarding our democratic processes and building public trust in our political institutions.

Recommendation: Remove the Political Exemption

[9] Vaile D (2018), 'Australia should strengthen its privacy laws and remove exemptions for politicians', *The Conversation*
[10] Worthington B (2019), 'Scott Morrison reveals foreign government hackers targeted Liberal, Labor and National parties in attack on Parliament's servers', ABC News

2.2 Protections

Transparency, Purpose Limitation and Data Minimisation
We strongly support the adoption of certain principles stipulated under Article 5 of the GDPR, in particular their determination that personal data collection and processing should be:

- Transparent
- Purpose Limited
- Necessary for the purposes for which they are processed

Under APP 3, an entity or organisation must not collect personal information unless the information is 'reasonably' necessary for its functions or activities. Now more than ever, the tech giants have direct and subsidiary business operations that span nearly every facet of industry. From healthcare to ecommerce, facial recognition to autonomous vehicles, the digital platforms have tendrils into every aspect that constitutes human work, life and play. An analysis by Brave exemplifies the scale of Google's operations, analysing over 100 documents that illustrate the data free-for-all within the Google ecosystem.[11] The pervasive power of the modern day tech giants makes this APP insufficient in safeguarding privacy.

Short of breaking up the platforms, the Privacy Act must adopt a purpose limitation principle that requires personal data to be collected for specified, explicit and legitimate purposes, and not to be processed further in a manner that is incompatible with those purposes.

Recommendation: Change APP 3 to ensure that personal information data collection operates under principles of purpose limitation

Further Incorporating a Rights-Based Approach
Whilst we recognise and appreciate the benefits that are imparted from principle-based regulation, the current approach has revealed significant gaps that struggle to contend with the complexities of modern data-driven systems. Whilst we support the ACCC's assertion that a wholesale adoption of EU GDPR might not be appropriate within the Australian context, incorporating elements of the European experience, in particular a rights-based approach with regard to their data subjects, can help ensure proper protection of Australians' privacy.[12]

There are many reasons why the additional adoption of certain rights to support the principles laid out under the APP will be beneficial. Firstly, enshrining certain rights related to privacy and data protection will serve to better future-proof this regulation in the face of a constantly changing digital landscape by setting a common reference point . Secondly, incorporating a rights-based approach will mitigate some of the issues around ambiguity, broad interpretation and unclear compliance requirements. And finally, granting these rights will engender more conscious conversations, norms and eventually cultures around privacy and data protection. This is especially important as our society grapples to not just deal with the numerous online harms the digital platforms have facilitated, but equip us with the vocabulary to grapple with

[11] Brave, 'Inside the black box: a glimpse of Google's internal data free-for-all', found online here.
[12] Regulation (EU) 2016/679 2016, Chapter 3

issues of emerging tech such as the future of work, bias in machine learning systems and artificial intelligence.

Recommendation: In particular, we support the incorporation of the following rights into our privacy framework. We highlight these four rights as they differ greatly from the current provisions in the Act, however strongly support the incorporation of other GDPR rights that have clear parallels with the APP.

- Right to Erasure, Article 17 GDPR
  The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay

- Right to Data Portability, Article 20 GDPR
  The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided

  We recognise the efforts that the Government is making through the Consumer Data Right however believe that these principles should also be enshrined within the Privacy Act.

- Right to Object, Article 21 GDPR
  The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her

- Automated individual decision-making, including profiling, Article 22 GDPR
  The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her

Ensuring the Privacy of Children

The average Australian teenager spends over 4 hours a day on the internet, with 1.5 being on social media.[13] The protection of children as they navigate within the digital world is of primary importance. Currently, companies and organisations are keeping Australian children under constant surveillance recording thousands of data points as they grow up. Everything from their location, gender, interests and hobbies, to being able to discern their moods, mental health and relationship status. This information is used to identify particular emotional states and moments where they are particularly vulnerable, in order to more effectively target and engage them.[14] Additionally, there have been documented cases, most notably Molly

[13] "Roy Morgan Single Source" by Roy Morgan (Oct18-Sep19)
[14] Darren Davidson, May 1, 2017, 'Facebook targets 'insecure' young people' *The Australian,* https://www.theaustralian.com.au/business/media/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6

Russell in the United Kingdom,[15] where these algorithmic systems have been shown to directly deliver harmful content that in Molly's case tragically resulted in her taking her own life. This illustrates both the horrific harms these platforms can facilitate and the specific vulnerabilities children face in navigating the online world.

Given that these algorithmic systems are fuelled by personal user data collected by the digital platforms under privacy terms of reference agreements, it is imperative we evolve this arrangement particularly for children. Obtaining a child's consent is complex, governed by a patchwork of common law and State-based statutes, raising questions on whether personal data of minors should be able to be obtained through the extractive surveillance practices of the digital platforms at all, and how we must construct a shared understanding and safeguards to ensure that these practices don't exploit vulnerabilities within children.

In the case that we do attempt to obtain informed consent on privacy from children, it is clear that this poses numerous challenges, but that these challenges must not result in weakened protections and/or rights. Specific considerations to create a supporting environment must be enacted for this consent to be informed and obtained legitimately.

Firstly, privacy terms of references, both through design decisions and language, create barriers for understanding especially for parents and children. Efforts must be made to present privacy policies not only in clear, plain and simple language but utilising the full suite of visual communication, UX and inclusive design techniques to ensure these implications are understandable.
Secondly, the expectation we have on parents and children to navigate this space without proper rights (such as the right to object and the right to erasure) makes the circumstances in which consent is offered problematic. These services provided by the digital platforms have become so ubiquitous, it is unreasonable and unrealistic to expect a child to 'opt-out'. Additionally, we are raising a generation of children whose every action, both foolish and otherwise, is recorded in perpetuity - without having the skills, norms and understanding to deal with these ramifications. This is why practices to 'obtain informed consent' must be situated in the context of broader digital and data rights protections.
Finally, specific expectations on the design of these services (such as privacy-by-design and data minimisation principles) must be enforced, recognising the specific vulnerabilities of children. The UK Government's development of the Age Appropriate Design Code[16] for online services, is a risk-based approach that enshrines fifteen standards that protect children within the digital world, and should serve as a strong benchmark for Australia to both adopt these learnings and develop a similar code. The code reflects much of the current Australian approach, such as defaulting to the most restrictive privacy and safety settings whilst additionally building on other protections (such as mitigating the effects of nudge techniques and geolocation).

[15] BBC News, 22 Jan 2019, 'Instagram helped kill my daughter', found at https://www.bbc.com/news/av/uk-46966009/instagram-helped-kill-my-daughter
[16] Information Commissioner's Office 'Age appropriate design: a code of practice for online services' 2020 found at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-0-0.pdf

Recommendation: Align the age requirement of a person to give their consent for the collection and processing of their personal information with the general rule under common law, that is that a contract or an agreement with a minor (under 18) is voidable. If a user is under 18, consent must be given by an authorised parent or guardian.

This consent must be supported through an enabling environment that includes: drastic changes to improve the understandability of privacy implications and agreements, granting of digital rights and the incorporation of specific expectations on digital services used by children, exemplified by the UK Age Appropriate Design Code.

2.3 Regulation and Enforcement

Resourcing and Enforcement

We strongly believe that the OAIC is underfunded and under-resourced, limiting the ability of the Privacy Act to be implemented and enforced. According to the Australian Privacy Foundation,[17] it currently takes the OAIC 6 months to act upon a complaint and according to the issues paper as of mid-2019, 10 out of the 12 Commissioner-instigated investigations from 2017-18 were still ongoing.

In addition to increasing the financial and technical capacity, the OAIC must be empowered with a spectrum of instruments so that it may guide APP entities and privacy practitioners. The reticence for Privacy Commissioners to hand down Determinations has left considerable ambiguity in how the Act and the APPs are to be interpreted. The OAIC must be given the license to issue a range of measures such as guidances, technical scopes and memos and expectation codes that range in their power to compel respondents to act. Additionally, whilst we support resolution through conciliation, there should be mechanisms to ensure that learnings and guidance from these instances are incorporated into our evolving public understanding of privacy, as well as avenues for recourse and appeal for complainants who have their complaints dismissed (this is expanded on under Direct Right to Action).

Recommendation: Consider a proportionate Privacy Levy that is committed to ensuring the adequate resourcing of the OAIC for the enforcement of the Act.

Recommendation: Consider expanding available instruments under s52 to empower the OAIC to provide appropriate guidance on Privacy Act and APP interpretation and implementation

Direct Right to Action

[17] Australian Privacy Foundation (2019), 'Submission to the Digital Platforms Inquiry'. Found online here.

We strongly support the proposal for a direct right of action that will provide individuals with the enforceable right to seek a determination from a court.

We want to emphasise that this is an alternative pathway, and that the role of the OAIC and the Privacy Commissioner must remain a primary pathway for complainants. However, this direct right to action will enable greater control over personal information and work towards ensuring individual data rights - a position we support. Litigation also improves transparency around our understanding of how the Privacy Act should be implemented.

As this alternative pathway opens up greater interpretation of the Privacy Act by the judicial system, we re-emphasise our recommendation on incorporating stronger rights-based protections detailed in our submission. This will ensure that these interpretations are built of a common understanding of privacy and data protection.

Recommendation: Grant the Direct Right to Action as an alternative pathway for individuals to seek arbitration on perceived privacy breaches and/or violations

Penalties

We strongly support the Government's decision to increase the maximum penalty for serious breaches of the act from ~$2.1 million to $10 million or three times the value of any benefit obtained through the misuse of information or 10% of the company's annual domestic turnover – whichever is the greater. Whilst we recognise that the penalty of 10% of the company's annual domestic turnover might have been included in order to capture Australian-operating APP entities, we believe that the most egregious breaches of this Act are and will continue to be by the major digital platform companies based overseas (in particular the United States). Even though Australia is a powerful signal market, we still make up a fraction of overall turnover for these global companies - as such, to ensure that a strong deterrence signal is sent, we strongly recommend changing that penalty to a % of the company's annual global turnover.

Recommendation: Change the maximum penalty for a breach to: $10 million or three times the value of any benefit obtained through the misuse of information or 5% of the company's annual global turnover, whichever is the greater

3.0 Conclusions

It is more important than ever to see privacy, not as a burden, but as our first line of defence in our efforts to ensure that current and emerging technologies work in the public interest. The review of the *Privacy Act 1988* comes at a time of extreme social change, as we grapple with unprecedented and existential challenges. This review must ensure that the Act is modernised to deal with these current issues, flexible enough to adapt to new threats and rooted in Australian values of social equity, autonomy and agency. The principles, rights and

protections afforded by this Act will lay our foundations as a society as we build out our understanding of digital rights and data protections in an age of disruption.