



**Australian
Privacy
Foundation**

<http://www.privacy.org.au>

Secretary@privacy.org.au

<http://www.privacy.org.au/about/contacts>

January 24, 2022

Privacy Act Review, Attorney-General's Department
Robert Garran Offices
4 National Circuit
Barton ACT 2600

Email: privacyactreview@ag.gov.au

Privacy Act Review - Discussion Paper October 2021

The Australian Privacy Foundation (APF) is the nation's preeminent civil society body concerned with privacy, namely community data protection, privacy, and information security expectations.

This third in a recent series of APF submissions about inquiries into Commonwealth privacy legislation¹ responds to the Privacy Act Discussion Paper.² We build on the Foundation's 6 December 2021 submission regarding the Exposure Draft of the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*³ and our substantial, November 2020 submission regarding *the Privacy Act Review – Issues Paper*.⁴

This submission draws broadly on submissions by the Foundation over the past two decades regarding systemic inadequacies in the national privacy framework, independent analysis by a range of entities including the Law Council,⁵ the Australian Law Reform Commission⁶ and other authoritative law reform bodies,⁷ and submissions from expert commentators (including current and former APF board members Anna Johnston and Prof Graham Greenleaf) and civil society bodies, noted at the end of this document.

¹ AustLII, Commonwealth Consolidated Acts, the Privacy Act 1988 http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/

² Australian Government Attorney General's Department. Privacy Act Review Discussion Paper, October 2021 (the Discussion Paper). <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/>

³ Australian Government Attorney General's Department. Online Privacy Bill Exposure Draft, 25 October 2021. <https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/>

⁴ Greenleaf, G., Waters, N. & Lane, K. et al. Bringing Australia's Privacy Act up to International Standards. (Australian Privacy Foundation Submission in Response to the Privacy Act Review - Issues Paper); 5 February 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3752152

⁵ Law Council of Australia. Submission; Review of the Privacy Act 1988 (Cth) Issues Paper, 17 December 2020. <https://www.lawcouncil.asn.au/publicassets/762d595e-dd59-eb11-9438-005056be13b5/3942%20-%20Review%20of%20the%20Privacy%20Act%20%20Issues%20Paper.pdf>

Law Council of Australia. Submissions, splash page on the Internet. <https://www.lawcouncil.asn.au/tags/submissions>

⁶ Australian Law Reform Commission (ALRC). Serious Invasions of Privacy in the Digital Era, ALRC Final Report 123, 2014; and For your Information: Australian Privacy Law and Practice, ALRC Final Report 108, 12 August 2008. <https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/>

⁷ ACCC. Digital Services Advertising Inquiry, Final Report, 2021; ACCC. Digital Platforms Inquiry, Final Report, 2019; and Productivity Commission. Data Availability and Use Inquiry Report, 2017.

General Observations

A human rights focus

A recurring theme throughout the Discussion Paper and this Review is that privacy (an inalienable human right which benefits individuals, families, communities and society in the public interest) is required to be ‘balanced’ with the interests of business and is necessarily subordinate to what is administratively convenient for government. This theme of subordination is wrongly over-emphasized and given unjustified priority. The foundation principle of the review should instead be that government agencies and business must work within, and indeed will benefit from, a coherent human rights framework. This is the approach (and must be) for all human rights, government and business.

The *Privacy Act* must be a comprehensive human-rights-focused law with a strong human rights protection and advancement aim. The current *Privacy Act* fails on this. This review must deliver (finally) a *Privacy Act* with a strong human rights focus: a clear priority that is no longer fundamentally weakened by concessions, exceptions and bureaucratic incapacity or lack of interest regarding enforcement.

It must include a statutory cause of action for serious invasion of privacy, something recommended by a range of law reform bodies over three decades — a remedy available in many other countries or areas of law, and one which would provide an effective recourse for individuals in instances where regulators fail to act in the public interest.

The Discussion Paper seems to take the view that there is “no right to privacy” as a human right⁸. This flawed approach is inconsistent with international human rights, and increasingly, with the expectations of Australia’s major trading partners. For example, the Office of the Australian Information Commissioner (OAIC) clearly states in its submission that “privacy is a fundamental human right”.⁹ We believe that the interpretation and approach of the OAIC is correct, and that the Discussion Paper has misinterpreted Australia’s international human rights obligations and wrongly discounted the centrality of recognising privacy as a right. In any event, regardless of arguments about interpretation of obligations, the *Privacy Act* must be effective rather than aspirational, and embrace a strong human rights focus as a counterweight to the endless demands from business and government for concessions weakening the position of individuals whose personal information (PI) is abused or misused. This is necessary to protect individuals in Australia, and to keep in step with evolving and strengthening privacy laws internationally.

Presumptions on interpretation

The *Privacy Act* is human rights protection legislation. This means that any interpretation or adaptation of this law should specifically favour an approach that strongly protects the privacy of people from the risks projected onto them by other powerful actors. The Act must contain a direction on this, as a specific section. This would assist in avoiding judicial decisions and administrative interpretations that in effect water down the effect of human rights legislation.¹⁰

This submission responds to most of the questions and issues identified in the Discussion Paper.

There are a lot of issues and questions. It is unclear if they are all intended as equally necessary or important. Not all are consistent with each other.

⁸ Discussion Paper, p.20

⁹ Submission by the Office of the Australian Information Commissioner: Privacy Act Review – Issues Paper, 11 December 2020, [Privacy Act Review Issues Paper submission - Home \(oaic.gov.au\)](#)

¹⁰ For example, the narrow definition in the Telstra IP case: *Privacy Commissioner v. Telstra Corporation Ltd* (2017) FCAFC 4.

For the avoidance of doubt, we consider the highest priority issues those in:

- 2.1–2.5 Definition of Personal Information
- 4.–7. Exemptions
- 9. Elements of Consent
- 10. ‘Fair and reasonable’ test
- 25.–26. Direct right of action and Statutory tort

Part 1: Scope and Application of the Privacy Act

1. Objects of the Act

Proposal 1.1

The proposed Objects in the Discussion Paper for the revised *Privacy Act* (the Act) unfortunately send a clear message to people in Australia that privacy should be completely subject to the interests and convenience of business and government.

The addition of the words “undertaken in the public interest” do not assist to protect people’s privacy.

Governments typically argue that everything they do is “in the public interest”, so such a qualification offers no effective benefit. Businesses will similarly simply argue that their activity is in the public interest. We remain very concerned that the Objects as drafted will send a clear message to any court to read down the privacy protections in the Act, and reinforce the reluctance of a range of regulators to address egregious data protection harms on a systemic or even a one-off basis. In fact, every document issued in reviewing the Act in this process supports a weak interpretation of privacy rights. We would be concerned that any finalised Explanatory Memorandum would continue to entrench this approach (noting that the Memo is extrinsic to the Act).

Proposal 1.1(b) must be removed.

Privacy rights must not be subordinated to government and business interests under a rubric of ‘balance’ or ‘public benefit’. Human rights must not be balanced with business interests. The right to privacy is about people having trust that personal information remains inherently private and being protected from abuse of that trust. The right to privacy attaches to every person in Australia; it is analogous to recognition of rights in the European Union, Canada and other jurisdictions where a justiciable Bill of Rights features privacy but has not eroded either public administration or economic development. Business must respect and work with the human rights of people in Australia. Any other approach (including ‘balancing interests’) leads to an ethical conflict of interest, since typically the empowered decision maker will be the beneficiary of an interpretation hostile to those rights. In effect, if business interests are preferred against the (human rights) interests of people, then the business would be acting against not only members of the public but its own employees. Business must act ethically, and proposal 1.1(b) is inconsistent with ethical business practice. The addition of ‘public interest’ does not resolve this ethical conflict (particularly considering the approach clearly articulated to ‘balance’ business interests).

Right to privacy

We reiterate our request (and support for the OAIC submission on this point) that the first Object needs to clearly recognise that people have a right to privacy. This must be the starting commitment for the Act. The right must be readily justiciable rather than a matter of lip service. Any failure to clearly state this Objective

sends a clear message to the Australian public that this review is about facilitating ongoing privacy breaches instead of protecting people's right to privacy.¹¹

In contrast, the EU *General Data Protection Regulation (GDPR)*¹² recognises the protection of rights and freedoms in relation to personal data (Article 1, Recital 1)¹³. The Privacy Act in Australia must take a similar approach. We would argue that this type of approach is necessary not only for maintaining the human rights of people in Australia but to ensure a level playing field for trade. Australia remains behind key trading partners such as the European Union; the EU continues to deepen and strengthen its privacy regime without detriment to national security, law enforcement or commerce.¹⁴

Public interest

We do agree that the public interest should be in the objects. However, it should be in the context of the protection of the right to privacy. In other words, the objects should specifically acknowledge that privacy protection reflects the public interest.

We recommend that the Objects cover:

- The right to privacy as a fundamental human right
- The public interest in privacy protection
- Interpretation that is beneficial to the individual, and acknowledges the Act is human rights protection legislation
- Consequent scope for people to take action to enforce those rights alongside the activity of regulators such as the Office of the Australian Information Commissioner, the Australian Competition and Consumer Commission and the Australian Communications and Media Authority.¹⁵

2. Personal information, de-identification and sensitive information

Proposals 2.1 – 2.4

We support a widely drafted and comprehensive definition of personal information. The proposed definition is generally a reasonable step in developing a workable definition.

We do recommend changes that are required to ensure that the definition does not create loopholes or inadequate protection.

- a. Remove “reasonably” in “reasonably identifiable”. It must be a question of fact on whether someone is identifiable or not. Once a person is identifiable the harm has happened regardless of any question of “reasonable”. In this use, “reasonable” serves to water down protection when the protections must favour the victim.

¹¹ We note that the Government has recurrently disregarded the Objects in the Freedom of Information Act, with statements by Ministers and key executives being reflected in day-by-day practice on the part of government agencies that is directly contrary to the presumption of access under that Act. On that basis the Objects in the new Privacy Act must be readily justiciable and the Act must not be fundamentally weakened through exclusions that render it not-fit-for-purpose at commencement or (given the history of creeping erosion) thereafter.

¹² General Data Protection Regulation (GDPR). <https://www.gdpr.eu/>

¹³ Recital 1. Data protection as a fundamental right, GDPR. <https://gdpr.eu/Recital-1-Data-protection-as-a-fundamental-right/>

¹⁴ We note hyperbole from some law enforcement representatives in parliamentary hearings over the past decade, including the unsubstantiated assertion that privacy law has reduced German police authorities to a laughingstock. The EU privacy regime has demonstrably not reduced Europe to anarchy; claims that it inappropriately hobbles law enforcement are at best disingenuous and should be publicly repudiated.

¹⁵ We specifically refer to the ACCC and ACMA because historically they have been more proactive in addressing privacy harms by practical action than the Privacy Commissioner/Office of the Australian Information Commissioner. We reiterate our concerns regarding the ongoing ‘balkanisation’ and ‘territorial fragmentation’ of privacy regulation at the Commonwealth level, with recent legislation enshrining a confusing set of bodies (such as the Ombudsman and Data Commissioner) alongside the OAIC and the Health Ombudsman and Privacy Commissioner. It is not helpful or respectful to Australians to have such a simple and central human right as privacy carved up and distributed over an ever-expanding range of different and inconsistent bodies, especially when Australians remain almost alone in the developed world in not having the right to sue to protect their own interests.

- b. The phrase “relates to” can be ambiguous and problematic in law and for privacy. If this phrase is to be used it needs further explanation and context. It must be defined very widely to avoid any narrow interpretation or causality implication. We support a wide definition that specifies that “relates to” includes not only anything about the individual but any information that concerns or may impact on the individual.
- c. We support a non-exhaustive list of the type of information capable of falling within the new definition of personal information. However, this non-exhaustive list needs to be carefully considered and comprehensive. In our experience, the non-exhaustive list is critical in providing guidance and direction to everyone. The proposed list is far too short and for example must include biometric data, inferred data, synthetic and other generated data.
- d. The proposed test for identifiability is manifestly inadequate. The phrasing is more towards protecting business (again) instead of creating a strong protection for the person who will experience harm if identified. We support the definition of identifiable as proposed by Salinger Privacy¹⁶ which is as follows:

Identifiable means:

If an individual is:

- (i) able to be identified directly or indirectly, or
- (ii) able to be discerned or recognised as an individual distinct from others, regardless of whether their identity can be ascertained or verified

Notes:

An individual will be ‘able to be identified directly or indirectly’ if there is more than an extremely remote or hypothetical likelihood of identification.

An individual will be ‘able to be discerned or recognised as an individual distinct from others’ if the individual, or a device linked to the individual, could (whether online or offline) be:

- i. surveilled, tracked, located, or monitored; or
- ii. profiled, contacted, or targeted to be subjected to differential treatment in the form of any action, decision or intervention including the provision or withholding of information, content, advertisements or offers; or
- iii. linked to other data which relates to the individual

- e. The definition of “collection” must also include the concept of inferred or future information. It is well understood that collection of personal information to build a profile is iterative.

Proposal 2.5

The definition of anonymous must be that the person cannot be identified ever. This definition does not work if there is any reference to identifiable. The definition must be factual – if it is possible to identify ever or in any way with technology then it is not anonymous. This is a very high bar. There is very substantial literature in the information science, health and law fields demonstrating that claims of ‘de-identification’ or

¹⁶ Salinger Privacy. Submission in Response to the *Privacy Act Review- Discussion Paper*, October 2021, 3 January 2022. https://www.salingerprivacy.com.au/wp-content/uploads/2022/01/22-01-03_Privacy-Act-review_Salinger-Privacy_Submission.pdf

‘anonymisation’ are generally overstated. It is very likely that all de-identified information can be re-identified now or in the future. It follows, that all de-identified information is not anonymous.

The definition of anonymous must meet a high bar because the legislation will no longer apply. If a strong definition of anonymous is not going to be used, then the legislation must still apply.

We would recommend a different approach. We would argue that the Act must apply unless the personal information has been deleted.

Proposal 2.6

We strongly oppose the Privacy Amendment (Re-identification) Offence Bill 2016. This Bill completely misunderstands the problem. The problem is that all de-identified data could be re-identified. Making it an offence only criminalises the people doing a public service and flagging the problem instead of dealing with the actual issue which is that the data could be re-identified, and privacy breached.

Deceased people

We do not support the Act applying to people who have died. We do acknowledge that there are practical issues that arise which may be able to be addressed in other ways. We refer readers to experience in the European Union.

Sensitive information

The definition of sensitive information should be updated to:

- Harmonise it with the definition of ‘personal information’; and
- Add in location data as sensitive
- Recognise that ostensibly ‘de-identified’ or ‘anonymised data’ may over time become more easily re-identifiable because of developments in i.e., data proliferation or data analytics tools

3. Flexibility of the APPs

Proposals 3.1 and 3.2

We support the ability for the OAIC to make an APP Code when required. The Code must be mandatory. Code making must be transparent and open to substantive public input, addressing concerns that part codes have been made behind closed doors. Code administration must be timely, transparent and efficacious rather than one bureaucratic hand languidly washing the other.

We would further support the OAIC’s recommendation for the power to intervene in a code development process by industry when required.

We would also strongly recommend developing detailed code standards that must be met to get a Code approved by industry. An example to consider is the ASIC Code approval process.¹⁷

Proposal 3.3 and 3.4

We support these proposals.

4. Small business exemption

¹⁷ Regulatory Guide 183: Approval of financial services sector codes of conduct. See [RG 183 Approval of financial services sector codes of conduct | ASIC - Australian Securities and Investments Commission](#)

We do not support the ongoing exemption for small business. It creates a huge loophole in privacy protections in Australia, one which may apply to c. 95% of all businesses. No other countries have an equivalent exemption. There is no basis for such egregious Australian exceptionalism. It is an international embarrassment.

Also of enormous concern is the “consent loophole” to deal with personal information for small business. This loophole is likely to be facilitating large scale data warehousing and consequent harms, including data breaches. As there is no effective auditing or overview of these practices it is safe to assume that this exemption is causing harm.

It is essential that this exemption is removed in this review.

5. Employee records exemption

The employee records exemption must be repealed. Employee personal information can be extensive and sensitive, particularly when integrated with other data and in environments where individuals are working on a networked ‘24/7’ basis. Employees are entitled to a right to privacy and should not lose basic protections when deciding to take a job.

We would also stress that with a workforce that increasingly works from home this exemption has become more problematic in the pandemic.

6. Political exemption

The political exemption must be removed urgently. The exemption is a matter of deep concern across the community. It may be administratively convenient but is not necessary or appropriate.

It is difficult to build trust of political parties when there is an exemption. People in Australia have the right to expect politicians to comply with the laws of this country rather than rely on exemptions. Large-scale data mining of voter characteristics (including integration with data from the dominant overseas profiling corporations) fosters both poll-driven – and media release-driven – public administration and results in the increasing community disengagement from political processes highlighted by researchers at the Australian National University and elsewhere.

7. Journalism exemption

The journalism exemption should be abolished and replaced with a limited exemption to conduct investigative and public interest journalism. This should be accompanied by detailed guidance, a complaints process (with free external dispute resolution) and sanctions for any breach.

We do not believe that self-regulation can work for journalism. It is a fragmented industry with very large players and small players, and continuing pressures to overlook traditional professional and ethical concerns in pursuit of personal ‘click-through’ targets.

Traditional claims that stronger privacy protection will cripple legitimate public interest investigations and standard reporting are self-interested and disingenuous. We for example note the vigour of journalism in Canada and Europe, both of which have more robust privacy protections and better options for enforcement than in Australia. One response to the corporate culture that saw egregious phone hacking by News

International, and more broadly a recurrent flagrant disregard of the personal lives of celebrities and nonentities alike, is that if journalists have done nothing wrong, they have nothing to fear.¹⁸

We note that the exemption has been traditionally most loudly advocated on behalf of outlets which confuse the concept of ‘the public interest’ with ‘what the public might be interested in, for a second’. These are more likely to resort to pointless ‘naming and shaming’ of easily-denigrated members of disadvantaged or unpopular groups in society than ‘speaking truth to power’ or other forms of investigative public interest journalism.

Recommendation:

Develop proposals to remove the small business, employee records and journalism exemptions.

Part 2: Protections

8. Notice of collection of personal information

Privacy notices do not work

We do support proposals 8.1. to 8.4 as detailed below. However, we stress that notices and particularly privacy notices are largely unread by people using any service. There is a very large empirical literature on this matter. Even with improvements in the notice and testing, people will remain unclear about what they were told. This makes privacy notices completely ineffective in any objective to inform people about the use of their personal information.

It follows that the only effective way to protect people from the misuse of their personal information is to set detailed standards about what are reasonable uses of personal information and what is not fair. This type of approach is the foundation of all human rights protection and consumer protection. The Act needs to not only improve the notices but decide what can go in the notices.

Proposal 8.1

We support this proposal.

We recommend that detailed guidance and consumer testing is needed to provide guidance to business on suggested approaches and minimum requirements for effective notice.

Proposal 8.2

We support this proposal.

We recommend adding a further point in the notice about whether a person can still get the service and refuse certain parts of the proposed use of personal information. The assumption that a notice removes the right to negotiate continues to reduce trust in the right for someone to control their personal information. We note concerns expressed by the Australian Competition & Consumer Commission in its major *Digital Platforms* report and corresponding studies from the United States, United Kingdom, Canada and other jurisdictions.

Proposal 8.3

We support standardised privacy notices which have been designed to be easily readable and present information in an accessible way.

¹⁸ We draw your attention to for example Ray Finkelstein and Rodney Tiffen, ‘When Does Press Self-Regulation Work?’ (2015) 38(3) *Melbourne University Law Review* 944.

Those notices must be readily enforceable. If they are not, they are, in practice, harmful, because they have only a rhetorical value.

Proposal 8.4

We support this proposal.

9. Consent to collection, use and disclosure of personal information

Proposal 9.1 and 9.2

We strongly support both the proposals as an improvement on the current situation.

However, as set out in our submission on the Issues Paper¹⁹ even with improvements, privacy consents are ineffective, and the proposed improvements are unlikely to provide protection. As already covered above, the only solution is to set up a framework of standard terms and ban unfair uses.

It is worth putting this in context. Consent is in effect an equivalent of the idea of ‘acceptance’ in traditional private law contract theory: there is negotiation, one party makes an offer, the other party accepts. This may have been state of the art in the 19th century age of ‘contract fundamentalism’, when there was an expectation that the parties were two gentlemen business figures, each able to look out for their own interests and come to a deal which suited both (and the role of the law was merely to ensure a remedy if one party breached the contract’s terms on their face). However the abuses that followed led in the 20th century to the blossoming of forms of law and regulation that recognised that a ‘signature on the dotted line’ (indication of consent) should not be the end of it. New laws on unfair contracts, consumer protection, credit and debt, fair trading and competition/anti-monopoly all recognised that the stronger party could often dictate unfair terms to the weaker party – who may not be in a position to understand or appreciate the terms of the deal, their implications (in part due to not having the same level of information access or analytic advice as the stronger party), or the issues of most detriment to their interests.

In the context of privacy law an undue focus or reliance on ‘consent’, while appropriate in some contexts, is problematic or unfair in many others. This is in no small part because the ‘terms of the deal’ are typically dictated unilaterally by the stronger corporate party (whether government or business) so there is power imbalance and scope for grossly one-sided provisions; and the nature of the material relied on to supply the ‘informed’ part of ‘informed consent’ is often – like consumer credit contracts before the advent of strong consumer protection law – impenetrable, incomprehensible, extensive, yet missing the key factual features which explain exactly who gets your information, how minimal are any limits on their use of it, and your (weak or non-existent) remedies if there is any abuse.

Many large online services operating in Australia from offshore promote the use of online contracts and consent as the basis for what can be quite privacy-hostile arrangements. Many governments also assume that they can use a ‘privacy policy’ to in effect oblige the individual involved, with no possibility of negotiation, to accept their terms and their effectively powerless position.

These problems with over-reliance on this form of privacy consent occurs at both the macro level of reliance of consent to impose unilaterally dictated terms hostile to the weaker party, and also the micro level, with various forms of what we might call ‘bad consent’, such as:

- ‘bundled’ or ‘coerced’ consent unreasonably requiring consent to diverse privacy and data risks which are not necessary to deliver the particular service, or specific to it;

¹⁹ Greenleaf, G., Waters, N. & Lane, K. et al. Bringing Australia’s Privacy Act up to International Standards. (Australian Privacy Foundation Submission in Response to the Privacy Act Review - Issues Paper); 5 February 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3752152

- ‘implied consent’ treating a certain action as if it meant the person had understood the terms of the deal; and
- ‘non-revocable consent’ which denies the person any escape if they later discover the true nature of the deal, the untrustworthiness of the entity, or particular negative implications for their own circumstances.

It is time to bring Australian privacy law protections up to par with the protections against consumers and citizens being improperly led to give consent to unfair or unconscionable contracts and anti-competitive abuses of market power, protections which have been found necessary to address market and administrative failures in other areas of business, commerce and government. The world economy has not stopped because these limits on reliance on ‘consent’ have been used to eg, over-ride waivers of one’s rights required in other forms of contract. And there is no reason to expect that innovative business or government entities could not adjust to an environment where the stronger party could not abuse the consent model for personal information dealings.

Where it is used, we support Greenleaf’s suggestion that consent cannot be validly obtained by deception, including the ‘dark patterns’ of interface design and software interaction which are widely used online.

10. Additional protections for collection, use and disclosure

Proposals 10.1 to 10.4

These proposals are strongly supported. Moving to a fair and reasonable framework is long overdue and the most effective protection of the right to privacy.

We do want to see a strong and effective fair and reasonable framework and we suggest the following changes:

- a. The framework overlays all the APPs and is included as a concept to consider interpretation of the Act
- b. A list of uses that are unfair and unacceptable (and are banned)
- c. Specific guidance for sensitive information and Government agencies where a higher level of trust is needed
- d. The list in proposal 10.2 is mainly a principles based approach. This can create interpretation arguments which result in practices that are privacy abusive. It is suggested that the principles be accompanied by standardised terms and approaches that requires fairness in practice.

We note that the Office of the Australian Information Commission in formally offering guidance about interpretation of the APPs has traditionally harmonised down rather than up. It is very concerning that the APPs embody a lowest common denominator approach.

11. Restricted and prohibited practices

Proposal 11.1: Option 1

We support a list of restricted practices because there is a high risk of substantive privacy harm (i.e. in terms of incidence and severity). We do not support option 2 as it would provide no protection.

We also agree with the activities listed as being high risk. We would argue that a better approach is detailed in the Salinger Privacy submission.²⁰

²⁰ Salinger Privacy. Submission in Response to the *Privacy Act Review Discussion Paper*, October 2021, 3 January 2022 pp 27-28. https://www.salingerprivacy.com.au/wp-content/uploads/2022/01/22-01-03_Privacy-Act-review_Salinger-Privacy_Submission.pdf

The main issue is to specify how these high risk activities will be regulated. We do not agree that the “must take reasonable steps to identify privacy risks and implement measures to mitigate those risks” is sufficient regulation of those high risk activities.

We recommend that the restricted practices trigger a process that includes:

Notification to the OAIC of the proposed restricted practice

An independent privacy impact assessment (PIA) that meets the OAIC guidelines

Review by the OAIC of the PIA

The OAIC has the power to require further measures to mitigate risk

The OAIC has the power to ban the restricted practice if it would lead to significant harm or is contrary to the public interest

If approved the APP entity must report on the implementation of the mitigation measures

We also strongly support a non-exclusive list of banned practices.

12. Pro-privacy default settings

Proposal 12.1 Option 1

We strongly support option 1 and oppose option 2 as it would be ineffective.

We would argue that this approach should apply to all privacy setting regardless of levels.

It is recommended that this proposal includes detailed guidance on pro-privacy settings in the Act.

13. Children and vulnerable individuals

No comment on proposals 13.1 and 13.2.

Vulnerable people

People can be vulnerable for a whole range of reasons. The vulnerability can be temporary or ongoing. Vulnerability can be caused by age, disability, violence, poverty, race, sex/gender, and the situation. As part of modernising the Act there needs to be a specific acknowledgement and provisions on vulnerability. We support consideration of this issue in the online privacy code, but it is also necessary to consider these issues in the Act.

The ACCC has done a large amount of work on this issue. The ACCC has published guidance *Don't take advantage of disadvantage*²¹ as a guide for business. The Competition and Consumer Act has unconscionable conduct provisions. The Act needs to have specific provisions and protection for vulnerable people. The provisions should include:

- Indicators of vulnerability
- Taking action to avoid taking advantage
- Remedies

We note the Government's emphasis on young people and other vulnerable people in the new eSafety Commissioner legislation and in protocols regarding implementation of that legislation. (We again express

²¹ Don't take advantage of disadvantage, 2011, ACCC at <https://www.accc.gov.au/publications/business-snapshot/dont-take-advantage-of-disadvantage>

concern regarding incoherence in Government policymaking, with the online safety legislation being fast-tracked – along with a range of national security legislation – ahead of the privacy review and resulting in practices that will foster large scale data breaches of potentially sensitive information.

14. Right to object and portability

Proposal 14.1

We support proposal 14.1.

If people cannot withdraw or revoke their consent, they do not have any real control of their personal information.

We would add that this proposal should be in the ‘consent’ part. Consent by implication includes refusal, withdrawal, and acceptance.

It must also be possible to limit consent for a time period because circumstances may change.

We oppose any personal information ‘portability’. We draw attention to concerns expressed by the Foundation over several years regarding the Consumer Data Right.

15. Right to erasure

Proposals 15.1 to 15.3

The right to erasure is really the crux of whether a person has control of their personal information. If there are serious limits and controls to the right to delete personal information, then this sends a clear message to the person that they really don’t control their own personal information. The current Privacy Act sends a clear message of a preference to privilege the convenience of business and government agencies at the expense of Australians. Contrary to recurrent statements by politicians, officials and corporate executives Australian in fact do not control the information about themselves and in law do not own that personal information. There is currently no right to delete. As we note below, in practice many Australians – including those with expertise and determination – encounter significant difficulty simply trying to ascertain what data is being held. Few have success in gaining a meaningful sense of how it is being used. Fewer still gain a sense, except through belated disclosures of data breaches (insufficiently deterred), about how data is stored, processed, protected and disposed of.

We support proposals 15.1, 15.2 and 15.3.

16. Direct marketing, targeted advertising and profiling

Proposals 16.1 to 16.4

We support these proposals.

Australians have consistently indicated that they find direct marketing burdensome and intrusive. Further regulation is required to manage this issue.

The main issue here is enforcement. Many people opt out of direct marketing just for it to pop up again. There is also an obvious sale of personal information across various marketing businesses.

Further regulation is required on top of the proposals to ensure that people have control over their interaction with direct marketing:

- a. A wide definition of direct marketing that reduces loopholes
- b. A ban on further contact after opt-out
- c. A simple and prescribed opt-out process with various options. Every person has experienced the opt-out that is impossible to access or make it work.
- d. Comprehensive jurisdiction. It is not up to the person to find what Act applies – the Privacy Act applies to it all.
- e. A penalty regime with clear fines for breaches

17. Automated decision making (ADM)

We do not support proposal 17.1. We have already stated that notice is generally ineffective; and notice alone can have the effect of implying the person affected understood and consented to the automated use of their data for decisions, when neither is true. The proposed notice would not be sufficient to deal with the issues raised, including those in submissions in footnote 898.

Alternative options to address the emerging risks, flaws and biases in ADM should be developed, taking into account the experience and evidence from examples like the long running ‘Robodebt’ fiasco, where debt collectors were commissioned to relentlessly pursue many social security recipients to ‘repay’ debts which were legally never owed, on the basis of defective ADM systems established by the Commonwealth and defended for many years.

Access as of right to critical information about ADM tools

It should not be necessary to litigate to discover the basis on which ADM is being used on you.

A more effective approach would be to require, as a reciprocal obligation, a high level of transparency from those proposing to carry out (inherently error-prone) ADM operations with personal information affecting the affairs of individuals: to require them to provide ready access to the algorithms, the training data set parameters and sample data, the specific operational data used for a particular decision about an individual which may be in dispute, and the test cases used to create and validate the ADM, to anyone who is or may be subject to their decisions, and their technical or legal advisers, as of right at no charge and without onerous process requirements.

This would be a way of making more practical the existing obligations in the Australian Privacy Principles about data quality including accuracy, completeness, currency and relevance (APP 10.2), as well as obligations in APPs 1, 5 and 12, so that the Act can address the otherwise obscure setting of use for ADM and offset the information imbalance that prolonged resolution of the Robodebt case.

AI should be deprecated as a descriptive term

We recommend that the term “artificial intelligence’ (AI) be avoided in this discussion.

It is a ‘framing’ term which elevates and overstates the level of sophistication of the technologies involved, and encourages excessive faith in the “intelligence” of what are however typically quite unintelligent pattern-matching tools prone to basic errors like confusing ‘correlation’ with ‘causation’, or reliance on flawed, incomplete, biased, irrelevant, inaccurate or out of date data sources.

Robodebt, for example, seems to have been implemented at the level of relatively simple traditional database operations relying on faulty and unproven assumptions in respect of various data sources, and flawed algorithms reliant on those assumptions.

Many other more sophisticated tools branded ‘AI’ are better described as ‘Machine Learning’ or ‘Neural Network’ tools, or similar more specific descriptors. While they can abstract statistical correlations and apparent patterns from large data sets in ways which may be then be useful for a very narrow category of decisions, they generally remain brittle, opaque, and complex to assess and trouble-shoot – especially from the perspective of a data subject denied access to key information and data. Acknowledging that their intelligence is just some form of pattern recognition, and providing access to information needed to assess its use in a specific case, as suggested above, will lead to more robust protection of personal information from misuse.

18. Accessing and correcting personal information

There are still problems with accessing and correcting personal information. The main problems are:

- a. It is not very clear how to ask. Finding the privacy policy can be difficult and most people do not know where to look.
- b. Some businesses just do not reply - requiring a complaint. The complaint can be difficult as well as the Privacy Act requires internal dispute resolution
- c. The process is not free. Cost or potential cost is a barrier.
- d. The information provided can be incomplete

We recommend further detail in the Act to address these issues including:

- Requirements on placement and accessibility on requesting access to personal information
- Making sure the Act specifically allows complaints for non-response
- Making the request free (at least if by email or electronically)
- Auditing by the OAIC and guidelines on improving storage and access.

Proposal 18.1

We support proposal 18.1 with the removal of disproportionate effort. The APP entity should be storing information in an accessible way.

Proposal 18.2

We object to this proposal. If the matter is in an external dispute resolution process that scheme can determine what may or may not be accessed. EDR schemes already do this when resolving complaints and will keep some information that it sees but not the complainant. The proposal as currently drafted just allows for the business to hide behind this exemption. It provides a ‘Potemkin village’ that is at odds with community expectations and with our comments above regarding the Objects of the legislation. It exacerbates the ongoing weakness of the OAIC.

We recommend that the exemption instead be that the EDR scheme would resolve whether the disclosure would be prejudicial. As the parties are already in EDR this would provide an independently decision so both parties can be satisfied with the fairness.

Proposal 18.3

This proposal is opposed. Again, this is providing exemptions and loopholes which are not necessary. It is up to the person accessing the information to decide on readability not the APP entity.

19. Security and destruction of personal information

Proposals 19.1 to 19.3

In general, we strongly support further measures to improve security and the safe destruction of personal information. The proposals, while an improvement, are inadequate.

The ongoing problems with data breaches, hacking and general problems with technology mean that this part of the Act must be modernised and future proofed. The legislation both can and must look ahead, given substantial independent research about emerging threats.

We recommend that:

- The Act include detailed requirements on security that must be met
- The OAIC guidance is updated
- A definition of destruction is included in the Act
- Organisations be incentivised by a deterrent that encompasses substantive financial penalties from the OAIC (similar to penalties from the ACCC under the Competition & Consumer Act) and scope for compensation under a statutory cause of action by entities that have experienced harm.

20. Organisational accountability

Proposal 20.1

We support proposal 20.1, but we consider it very weak.

We support the OAIC proposals and support them being included in the Act.

We would also recommend a ‘privacy by design’ approach be included.

21. Controllers and processors of information

We do not have a developed view on the questions on p 158.

It is notable that submissions on this topic came mostly from industry associations and large online businesses, rather than from advocates for the interests of individuals affected. In any discussion on this it would be important to identify potential impacts on individuals and data subjects, including in the context of other changes proposed in this review. The heading ‘Challenges of introducing these concepts into the Act’ does not appear to explore this in the same depth as it considers the benefits; it should do this more robustly.

Any proposed change should be cautious about providing a basis for an entity dealing with personal information to deny responsibility for their role in any adverse effects.

Harmonising

While there may be benefits in harmonising with international approaches, as suggested in submissions in footnote 1056, from the perspective of individual Australians affected by use of their personal information it would be better to start harmonising with the more important things such as direct right of action and statutory tort, consent, definitions and exemptions; and given that full harmonisation is not viable and choices have to be made, also to avoid weakening any local protections in the process.

(It does not seem appropriate to flag harmonisation as a justification for relatively minor changes, of interest to some data handlers, when the more important comparative matter is Australia's lack of effective enforcement options for individuals, in stark contrast to most of the relevant jurisdictions.)

22. Overseas data flows

Proposal 22.1–22.6

The key issue with these proposals, from the perspective of the interests of the individuals whose data may be sent out of the jurisdiction, is to avoid losing the benefits of the existing obligation on the entity doing the exporting, both since they are in practice responsible for the decision and the outcomes of their decision, and since they are within jurisdiction and more easily subject to efforts from the affected person to obtain redress.

Many of the proposals here have potential to make it harder for the individual adversely affected to use Australian law in a simple and direct way to enforce their rights. While we do not necessarily strongly oppose every proposal here, we cannot support them without recognition of what's at stake and frank acknowledgement of the difficulties they may create for individuals seeking justice in Australia.

It may be understandable that such entities may wish to escape liability and to outsource this obligation, but it will generally not be appropriate for the Act to facilitate this any more than at present. (There is already a loophole where they get such a benefit if they believe the foreign regime is adequate, even when in fact it turns out not to be.)

This will be even more important when the private right of action and the statutory tort are finally implemented in Australian law, since trying to exercise such rights in another jurisdiction will be difficult, expensive and uncertain.

Standard Contractual Clauses (SCCs)

There is reference to use of Standard Contractual Clauses (SCCs) as a mechanism. While contracts set out expectations of a foreign data recipient, and this is a necessary aspect of a data export activity, it is critical to keep in mind that almost always the data subject, the individual affected, is not a party to such a contract and cannot enforce them or address a breach.

Therefore the weight given to SCCs should be limited, and their potential to relieve a local entity of obligations should be avoided because to do otherwise is to weaken the capacity of the Australian involved to protect their own interests from abuse offshore.

Adequacy

We support in general the efforts to seek an adequacy ruling from the EU.

Most of the proposals we make in this submission will support or be necessary for such a ruling, especially in relation to exemptions, and to the data export issues flagged above – another reason to exercise caution in facilitating local entities avoiding responsibility for consequences they put in chain by exporting data.

Schrems II

Another matter for the EU to consider is whether Australian governments will have access to imported personal data about EU citizens in ways which will contravene the interpretation of the GDPR in the Schrems II case. The extensive intrusions faced by Australian citizens and others affected by the relentless expansion of these police and intelligence service powers over the last two decades may not be compatible with this key ruling.

It is disappointing not to see this central issue in transborder personal data flows from Europe not discussed in the DP, since it has been controversial for most of the last decade.

23. Cross-border privacy rules and domestic certification

Proposal 23.1

We do not support this proposal.

We concur with Prof Greenleaf's conclusion, based on close observation of its history, that the APEC Cross-border Privacy Rules scheme (CBPRs) is dead and should remain so. The description of this CBPRs as 'an international certification scheme with well-established enforcement mechanisms' is not correct, given there are no examples of the supposed enforcement mechanism ever having been used anywhere, and that such schemes cannot deliver remedies to individuals.

In addition, their use may put at risk 'adequacy' assessments from e.g., the EU.

Proposal 23.2

We do not support this proposal.

The APEC CBPRs is not compliant with Australian law but implements the much weaker APEC Privacy Framework. Anything based on it would not be compliant with Australian law, so it is unclear why one would propose a local certification scheme on this basis.

Part 3: Regulation and enforcement

24. Enforcement

Proposals 24.1 – 24.9

We strongly support all the proposals from 24.1 to 24.9 (option 1).

We support the OAIC having sufficient powers (including own motion investigative powers) to ensure appropriate enforcement. Powers in themselves are inadequate; it is important that they are used on a timely and transparent basis (encouraged by an OAIC culture that has regard to the Objects we note above).

It is particularly important that the public has confidence that the OAIC has all the powers, resources and culture needed for remedies including redress for the person harmed by the privacy interference. The OAIC must have the power to prevent future loss as this is part of preventing ongoing harm.

We strongly support an industry funding model for the OAIC to ensure it is adequately funded to perform its role as a regulator. We note however concerns with other regulators, for instances substantive criticisms that the industry-funded Therapeutic Goods Administration has been captured by the businesses it is meant to regulate.

Section 41 complaints reporting is important. We have experienced (and had reports) of many substantive privacy complaints (including systemic "class action" type complaints) being discontinued under section 41 of the Privacy Act. In our view, the OAIC has an ongoing and problematic conflict of interest between its role as regulator and as a complaint handling body.

No other regulator in Australia is a complaints handling body. A complaints handling body needs to be independent and the OAIC is not independent.

We strongly support moving to an EDR model for privacy complaints. The Australian Financial Complaints Authority (AFCA) already handles a range of credit reporting and privacy complaints. Many businesses are already members of an EDR scheme. A separate EDR scheme could be set up if needed but we would prefer a separate section of an existing EDR scheme deal with privacy complaints. IN our experience it can take some years for an EDR scheme to mature into an effective complaints handling body.

The key advantages of moving to a separate and independent EDR are:

- a. The EDR scheme has considerable expertise in resolving complaints
- b. Systemic issues can be referred to the OAIC
- c. EDR is user friendly and works on accessibility (for example taking complaints over the phone)
- d. There is specific assistance for vulnerable people (escaping DV, Aboriginal and/or Torres Strait Islander people, Difficulty with English (providing translations), disability etc)

Using an EDR scheme would require revision of the Act to:

- Mandate EDR membership
- Deal with failing to be a member
- Remove OAIC as a decision maker
- Amend the time limit which is currently a too short 12 months to the standard 6 years that EDR uses
- Deal with systemic issues
- Work out a process for “class action/representative/test case” complaints
- Work would be needed to ensure that privacy breaches can be dealt with as a direct loss (without no obvious monetary loss)

25. A direct right of action

This proposal is strongly supported. It is fundamental. It does not prevent efficient (as distinct from politically and bureaucratically convenient) public administration, law enforcement and journalism

The right of action would benefit both people and business by clarifying the law judicially and in EDR.

The only extra recommendation we would make is for a mechanism for a right of action complaint to go directly to court if it is systemic and involves a class of people.

We consider that the right of action is salient given the absence of a justiciable constitutionally-enshrined Bill of Rights (disquietingly, Australia remains the only major liberal democratic nation without such a Bill), the inadequacy of legal aid funding, the politicisation of the Administrative Appeals Tribunal and the reluctance of the Government to institute a Commonwealth integrity commission.

26. A statutory tort of privacy

We strongly support proposal 26.1 – option 1. We support the Australian Law Reform recommendation in its Report 123.

Our view is also that it is highly desirable that the privacy right of action be clearly defined as a statutory tort, to embed it within an established branch of law. Our longstanding policy remains in place:

- a. it must be available to individuals, but not to ‘legal persons’ such as companies

- b. it must enable a court to grant injunctions, award damages, and impose penalties and exemplary or punitive damages
- c. it must require the court to balance the privacy interests of the litigant against other important interests, including and especially ‘the public interest’
- d. it must provide a clear framework and criteria for evaluating a defence that an invasion of privacy is justified in ‘the public interest’.

27. Notifiable data breaches scheme – impact and effectiveness

Proposal 27.1 is support but it is insufficient. We still support the amendments recommended (63 to 66) by the OAIC in its submission in response to the Issues Paper.²² Those recommendations must be enacted to make the scheme work more effectively.

As it stands, the notifiable data breaches scheme works just to notify but does not result in any real changes or remedies for people. We would classify it as very ineffective legislation.

28. Interactions with other schemes

We support proposal 28.1 to 28.3.

Errata

On page 5 there is a reference to the APC - Australian Privacy Council. This should presumably be the Australian Press Council, as there is no Australian Privacy Council (though APF is sometimes misattributed this way).

Other submissions

The APF endorses the important Salinger Privacy submission²³ mentioned in this response. In particular strengthening and clarification in the following areas are most important:

- 2.1–2.5 definition of ‘personal information’
- 9. elements of consent
- 10. ‘fair and reasonable’ test

We also endorse the submission from Professor Graham Greenleaf,²⁴ particularly his concern for the ‘elephant in the room’, ‘Australia’s scandalous wholesale exemptions from the scope of the Act’:

- over 95% of businesses via the ‘small business’ exemption;
- use of personal information in employment (affecting everyone who has some form of traditional job);
- use of PI by political parties (each election season seems to generate a new form of abuse of the personal information of potential electors, most recently SMS spam);
- journalism (see above);
- public sector uses such as by police and intelligence (leading to a lack of clarity about the principles which should apply to surveillance, interception, retention and investigatory powers); and

²² Submission by the Office of the Australian Information Commissioner: Privacy Act Review – Issues Paper, 11 December 2020, [Privacy Act Review Issues Paper submission - Home \(oaic.gov.au\)](#)

²³ Salinger Privacy. Submission in response to the *Privacy Act Review Discussion Paper*, October 2021, 3 January 2022. https://www.salingerprivacy.com.au/wp-content/uploads/2022/01/22-01-03_Privacy-Act-review_Salinger-Privacy_Submission.pdf

²⁴ Greenleaf, G. Submission in response to the *Privacy Act Review Discussion Paper*, October 2021, 30 January 2022

- ‘publicly available information’ (which can operate to legitimise abuses ‘after the fact’: once PI has been made available by whatever means, fair or foul, it is open to the claim of this exemption).²⁵

Conclusion

The *Privacy Act* needs to be enlivened to better support the growing expectations of Australians, and people and businesses in other countries, that the fundamental human right to privacy will not be conceded away or undermined in Australia by continuing the current approach: one which favours hostile claims by corporate and government entities (which do not themselves suffer from abuse of personal information), and which offers enforcement which is weak, fragmented and ineffective by comparison to other consumer or citizen protection laws in Australia, or to privacy laws in other comparable countries.

We would be happy to assist with the formulation of workable privacy legislation that fosters a growing community trust in national privacy protection and implementation of fit-for-purpose remedies.

Yours sincerely

David Vaile, chair
Australian Privacy Foundation
enquiries@privacy.org.au

Acknowledgment

I acknowledge and thank the members of the APF Board, especially Kat Lane, for their guidance herein.

²⁵ We would add the concept of ‘expectation’, hypothetically illustrated by an assertion such as: ‘another minister has trashed a critic’s partner’s personal information privacy in the past without rebuke or enforcement, so you should have expected that public criticism of perceived maladministration would lead to your partner being doxxed too’. This is potentially another method of legitimising unpunished privacy abuses after the fact, raising the threshold of what counts as abuse in future and in effect compounding the significance of individual abuses.