# Submission to the Attorney-General

on the Discussion Paper regarding the

# Review of the *Privacy Act 1988*

10 January 2022

# Overview

We welcome the opportunity to submit comments to the Attorney-General concerning the review of the Privacy Act 1988. Digital Rights Watch has been actively following the development of privacy legislation in Australia, and we have been particularly interested by the findings of the ACCC inquiry into Digital Platforms and its extensive emphasis on the need for privacy and data protection in order to protect consumers in the digital era.[1]

We are concerned about the concurrent effort to regulate online privacy through the Online Privacy Bill (OP Bill), which threatens to create a two-tier system for privacy protections in Australia based on age. We strongly urge the government to pursue updating the Privacy Act as a matter of priority and urgency rather than developing competing regulations, in order to create the safeguards all Australians desperately need in the digital ecosystem.

There are also several other simultaneous regulatory efforts which threaten to muddy the impact of the new Privacy Act by creating confusion and too many parallel mechanisms for individuals to engage with. Some of our submissions relevant to the topics covered:

- Data Availability and Transparency Bill (November 2020) https://digitalrightswatch.org.au/2020/11/12/submission-the-data-availability-and-transparency-bill/
- Privacy Act Review Issues Paper (November 2020) https://digitalrightswatch.org.au/2020/11/27/submission-privacy-act-review-issues-paper/
- Online Privacy Bill (December 2021) https://digitalrightswatch.org.au/2021/12/07/submission-online-privacy-bill/

## Digital Rights Watch

Digital Rights Watch is a charity organisation founded in 2016 whose mission is to ensure that people in Australia are equipped, empowered and enabled to uphold their digital rights. We stand for Privacy, Democracy, Fairness & Freedom in a digital age. We believe that digital rights are human rights which see their expression online. We educate, campaign, and advocate for a digital environment where individuals have the power to maintain their human rights.[2]

[1] The ACCC Digital Platforms Inquiry final report provides several recommendations on how to strengthen the rights of consumers in the digital space, including stronger privacy protections and data rights: https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report
[2] Learn more about our work on our website: https://digitalrightswatch.org.au/

# Summary of Recommendations

**Recommendation 1**
Introduce a federal level right to privacy in order to effectively empower all Australians in the digital age and protect them against privacy violations by public and private entities.

**Recommendation 2**
We support a direct right of action under proposal 25, including civil penalties as well as damages that can be awarded to the individual complainant.

**Recommendation 3**
Introduce a statutory tort for invasions of privacy.[3] Establishing a statutory tort for invasions of privacy would greatly extend individuals' ability to exercise their rights and keep entities processing their data (public or private) accountable. Of the four options presented under proposal 26, we are in favour of Option 2.

**Recommendation 4**
Explicitly include language in the definition of personal information to ensure that "identifiable" includes the notion of "distinguished from others even if the identity is not known" (i.e. include the notion of individuation not just identifiability).

**Recommendation 5**
Include inferred or generated data in the definition of "personal information", in addition to using it as an example of the act of collection.

**Recommendation 6**
Adopt the "extremely remote or hypothetical risk of identification" test proposed for the definition of "de-identified" to apply to the definition of "identifiable", to remove ambiguity around what does and doesn't constitute de-identified data.

**Recommendation 7**
Remove proposal 2.6 which would have a detrimental impact on research.

**Recommendation 8**
Ensure the definition of "sensitive information" aligns with the new definition of personal information, including a change from "about" to "relates to", as well as inclusion of information that is generated, inferred, or can otherwise act as a proxy for sensitive information. Consider introducing a "reasonable suspicion" test such that if an entity could or should have had a reasonable suspicion that certain personal information could be used as a proxy for sensitive information, it should be treated as sensitive information under the Privacy Act.

**Recommendation 9**

[3] The creation of a tort for serious invasions of privacy was already recommended by the Australian Law Reform Commission in 2014, since then the need for such an avenue has increased as data harvesting practices are skyrocketing in Australia. It was further suggested in the final report of the ACCC's Digital Platforms Inquiry.

Strengthen the meaning of consent as in proposal 9.1. We further suggest that the definition of consent should also clarify that consent is not permanent or ongoing, and can be withdrawn.

**Recommendation 10**
Consent shouldn't be used as a way to circumvent complying with purpose limitation and other limits and protections. For consent to be meaningful, it needs to be provided as a result of a genuine choice that is made from a position of knowledge. It must not become a transactional, box ticking requirement, that then serves as a licence to use personal information without limit.

**Recommendation 11**
Include standard requirements to allow people to opt out of all collection of information that is not essential to the technical functionality of a service.

**Recommendation 12**
Refine the list of legislated factors under proposal 10.2 to narrow the scope of what might be disingenuously argued to be "fair and reasonable". We suggest that this may include considering a hierarchy or weighting of legislated factors, for instance, that business interests should always be weighted far less than the best interests of a child.

**Recommendation 13**
Clarify further that the fair and reasonable test is a *threshold* test, and that if that test for an activity is failed, entities cannot use another ground for the practice.

**Recommendation 14**
Introduce a qualifier to point 4 of the legislated factors under proposal 10.2, so that the "fair and reasonable" test requires the functions and activities of an entity are balanced with how those practices impact or undermine the fundamental rights and freedoms, autonomy, or interests of an individual.

**Recommendation 15**
The OAIC should offer guidance regarding how to satisfy the fair and reasonable test in practice, including examples of practices that would *not* be considered fair and reasonable. This would allow some flexibility to adapt the test to the evolving nature of digital technologies.

**Recommendation 16**
We support the introduction of restricted practices. Such activities should trigger a requirement for APP entities to implement additional protections and organisational accountability measures (Option 1 under 11.1), rather than relying on an individual privacy self-management approach (Option 2).

**Recommendation 17**
A small number of prohibited practices should be introduced which represent unreasonable risk of harm and undue interference with privacy. We recommend that one-to-many facial recognition be included in this list.

**Recommendation 18**
Entities that handle personal information relating to children should be subject to additional obligations to embed additional privacy protections, such as restricting secondary use of personal information of children.

**Recommendation 19**

The Privacy Act must apply to any and all entities which collect, process, or otherwise handle personal information. The flexibility of the APPs already allow regulated entities to take a risk-based approach based on their particular circumstances, including size, resources, and business model. Therefore the compliance costs would be commensurate with their risk profile.

**Recommendation 20**
Provide small businesses with additional, targeted resources and support to adopt the privacy practices required by the Privacy Act. Additional funding to the OAIC or another entity should be provided to make this possible.

**Recommendation 21**
Remove the political exemption as a part of reviewing the Privacy Act.

**Recommendation 22**
Remove the employee records exemption, or, commit to standalone workplace surveillance legislation.

**Recommendation 23**
Further investigate existing workplace surveillance practices across Australia to identify what is needed to adequately protect workers' rights; balancing digital privacy of workers with reasonable monitoring requirements within an employment relationship, and the ongoing impacts of the COVID-19 pandemic with regard to the extension of workplace monitoring into personal environments.

**Recommendation 24**
Introduce a public interest test to the journalism exemption, such that it will only apply where journalism is in the public interest. The public interest test should include consideration of the rights of the individual.

**Recommendation 25**
Extend the application of APP 11 on data security to media organisations.

**Recommendation 26**
Breaches of the APPs should give individuals the right to bring a case in court (not just to the OAIC), including as representatives of a class. For such cases, there should be a regime of civil penalties for breaches of the APPs that can be awarded to the individual.

**Recommendation 27**
Further consideration ought to be given to the development of provisions which give individuals a meaningful and accessible pathway to seek an explanation, audit, and review of decisions made by automated means. This should also include attribution of the automated decision to the entity that used the automated system, and compensation for any harm caused by an incorrect decision made by automated means.

# General remarks

At Digital Rights Watch (DRW), we are equally concerned about the lack of a federal level protection for privacy as a human right as we are about the ever growing collection and use of personal data by public and private entities. Throughout the ongoing review of the Privacy Act, we have urged the government to focus on addressing the most pressing systematic data collection and exploitation models that digital platforms, data brokers, and targeted advertisers thrive on—and ensure meaningful protections and actionable rights for individuals.

As a result of the COVID-19 pandemic, we have seen our lives move increasingly online as many work, study and interact remotely with friends and families. The emphasis on technology was unprecedented across education sectors and remote workplace teams, and a lack of strong privacy safeguards left many Australians frustrated and questioning their rights and liberties.[4] At DRW, our concern has grown over the unchecked predatory data collection and aggregation practices of many digital services and Internet platforms, many of which have become an unavoidable—if not outright mandatory—fixture in people's everyday lives. Updating the Privacy Act has the potential to give Australians the ability to better control how their information is used and shared, and empower them to take action when their privacy is violated. At the moment, internationally, we are falling behind in addressing privacy challenges, as well as the broader socio-economic harms caused by the data extractive business models of digital platforms and services.

**We believe that recognising the right to privacy at the federal level is critical to protecting the privacy of all Australians.** Enshrining a right to privacy within the Privacy Act would create a rights-based relationship with the way Australians' data and privacy is treated online, as opposed to an economic or value-driven model which has been the case so far.[5] While other amendments to the Privacy Act will play a key role in improving the protections against arbitrary infringements upon Australians' privacy, without a right to privacy the impact of the reforms made to the Privacy Act will remain limited. DRW is of the view that Australia needs a comprehensive federal charter of human rights, but until this is realised, introducing a right to privacy in the Privacy Act is essential.

Similarly, a statutory tort would be a welcome improvement, although it is only a partial substitute for implementing the right to privacy as a stand alone right, without the need to meet the requirements of the tort. **It is our view that in order for privacy protections to be meaningful in Australia, there is need for all three of these changes: a federal right to**

---

[4] Technology and Power: Understanding issues of insecure work and technological change in Australian workplaces, August 2020, *United Workers Union*. Available at: Technology-and-Power-UWU-Submission.pdf (united workers.org.au)

[5] The emphasis on Consumer Data Rights (CDR) is evidence of this, as is the consideration by the Australian Bureau of Statistics to merge privately held datasets into the public census data to improve results and the "economic contribution" of the census. This value-driven calculation of privacy infringement vs economic benefit fundamentally shifts when we consider a rights-based system.

**privacy, reform to the Privacy Act, and a statutory tort for serious invasions of privacy.**

As a part of reviewing the privacy ecosystem in Australia, we therefore urge the government to enshrine in law a federal level right to privacy in line with Article 12 of the United Nations (UN) Universal Declaration of Human Rights, to which the Australian government is a signatory. Article 12 states: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks”.[6] Article 12 is well established and recognised around the world, and Australia is a signatory to the UN Universal Declaration of Human Rights. This would bring Australia into line with comparable jurisdictions and, for this reason, align with community expectations.

Any such right should be actionable in court. One of the key components of a functional privacy or data protection regime is the ability for individuals’ rights to be enforced and for individuals to seek remedy.

We acknowledge that proposal **1.1(b)** to amend the objects in section 2A goes some way toward rebalancing the perception of privacy away from a value-based model by recognising that the protection of privacy of individuals should be balanced with the interests of entities in carrying out their functions or activities *undertaken in the public interest.* This is a welcome improvement, however, it should only be the starting point. Privacy, as a human right, should not be treated as a bargaining chip in the economy that can be taken in or out of the game according to profit-driven or economic interests.

**Recommendation 1**
Introduce a federal level right to privacy in order to effectively empower all Australians in the digital age and protect them against privacy violations by public and private entities.

**Recommendation 2**
We support a direct right of action under proposal 25, including civil penalties as well as damages that can be awarded to the individual complainant.

**Recommendation 3**
Introduce a statutory tort for invasions of privacy.[7] Establishing a statutory tort for invasions of privacy would greatly extend individuals’ ability to exercise their rights and keep entities processing their data (public or private) accountable. Of the four options presented under proposal 26, we are in favour of Option 2.

---

[6] Universal Declaration of Human Rights, *United Nations*. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights

[7] The creation of a tort for serious invasions of privacy was already recommended by the Australian Law Reform Commission in 2014, since then the need for such an avenue has increased as data harvesting practices are skyrocketing in Australia. It was further suggested in the final report of the ACCC’s Digital Platforms Inquiry.

## Definition of "personal information"

We are pleased to see proposals included in the *Discussion Paper* to re-draft the threshold of "personal information". The definition of personal information has acted as a gatekeeper to the protections offered by the Privacy Act for too long, so this is a welcome change, and aligns with our initial recommendation to the *Issues Paper*.

We generally support proposals **2.1**, **2.2**, and **2.4** with regard to the expansion of the definition of personal information, including amending the wording from "about" to "relates to", which will address much of the confusion regarding protections offered to technical data caused by the *Grubb v Telstra* case. We do suggest, however, that additional explanation of what "relates to" means be included, to avoid possible future judicial determinations that might interpret the scope of "relates to" in an overly narrow way.

We are also pleased to see the *Discussion Paper* state that the intention is to "cover circumstances in which an individual is distinguished from others or has a profile associated with a pseudonym or identifier, despite not being named".[8] This would play an important role in ensuring that entities cannot evade regulation by claiming that they do not know who the individual is. By now it is well known that the harms caused by targeted advertising and data brokers have little to do with the ability for companies to associate an identity to individuals. With enough data, companies are able to determine individuals' social, political, and economic preferences, to create a kind of "abstract identity".[9] It is essential that the Privacy Act offers protection for cases of individuation, not just identifiability.[10]

To this end, we also question the reliance on "reasonably" identifiable in proposal **2.3**. The inclusion of the "reasonably" qualification upon identifiable weakens the scope of the definition, and makes Australia out of line with privacy law around the world, including the European Union's General Data Protection Regulation (EU GDPR) and similar laws in New Zealand, Canada, Singapore, and Japan, among others.

There also appears to be a gap between the test arising from the proposed definition of personal information - "reasonably identifiable" - and the proposed definition of de-identified data - "extremely remote or hypothetical risk of identification". This means that it is possible that data may fall in the gap where it is not "reasonably identifiable" and therefore does not fall under the definition of personal information, and simultaneously does not meet the test for what would be considered de-identified data.

In our recent submission regarding the Online Privacy Bill we highlighted that many social media companies and data brokers benefit from being able to consider their activities as falling outside the scope of the Privacy Act, largely due to the concept of being "reasonably

---

[8] Privacy Act Review Discussion Paper, page 27.
[9] 'Future Histories', *Lizzie O'Shea*
[10] See 'Individuation—Re-thinking the scope of privacy laws', *Salinger Privacy,* 30 August 2016, available at https://www.salingerprivacy.com.au/2016/08/30/individuation/

identifiable".[11] For example, LiveRamp (formerly Acxiom) states that they perform "data anonymization" because they remove all personally identifiable information.[12] This means that, while readily understood to be privacy-invasive, the practices of such companies would likely not be required to handle such aggregated data in accordance with the Privacy Act. This is a concerning gap in protections for Australians.

We are pleased to see that proposal **2.4** suggests expressly including information that is generated or inferred. While the OAIC has previously issued guidance in alignment with this regarding "collection via creation", explicit inclusion of this within the Privacy Act would be a welcome improvement.[13]

Inferences, predictions, or other assumptions made about people based on the data collected about them can have very real negative consequences, and should be considered as a form of privacy harm. A failure to include generated or inferred information within the scope of the Privacy Act would represent a failure to acknowledge the modern technical realities of data processing.

Personal information that is generated or inferred, by way of machine learning or other techniques, should also be contained in the list of information under proposal **2.2** to avoid the possibility of entities attempting to argue that generating or inferring information *after* the point of initial collection is a "use", rather than another point of collection. We note that in Facebook's submission to the *Issues Paper* they argue that the information they infer about people is not and should not be regulated as personal information.[14] This would only serve their business model and not the protection of individuals' rights. Given the demonstrated scope of downstream harms that can arise based on inferences made on personal information, this kind of derived information is worthy, and in need of, legal protection.

**We emphatically do not support proposal 2.6 to re-introduce the re-identification offence bill.** The initial proposal to criminalise re-identification of de-identified data released by public sector organisations was met with very serious and legitimate concern that doing so would lead to penalising researchers and white hat hackers who play a fundamental role in identifying security weaknesses, and would ultimately act as a deterrent for public interest research. Rather than criminalising re-identification, effort would be better spent to ensure that the security and privacy of the data released by public sector organisations is a matter of priority.

---

[11] Submission to the Attorney-General on the proposed Online Privacy Bill, *Digital Rights Watch,* December 2021. Available at: https://digitalrightswatch.org.au/2021/12/07/submission-online-privacy-bill/

[12] See LiveRamp Security and Privacy details: https://liveramp.com/our-platform/security-privacy/

[13] 'Guide to data analytics and the Australian Privacy Principles', *Office of the Australian Information Commissioner,* 21 March 2018, available at: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles

[14] Submission to Australian Privacy Act Review Issues Paper, December 2020, *Facebook.* Available at: https://www.ag.gov.au/sites/default/files/2021-02/facebook.PDF

**Recommendation 4**
Explicitly include language in the definition of personal information to ensure that “identifiable” includes the notion of “distinguished from others even if the identity is not known" (i.e. include the notion of individuation not just identifiability).

**Recommendation 5**
Include inferred or generated data in the definition of “personal information”, in addition to using it as an example of the act of collection.

**Recommendation 6**
Adopt the “extremely remote or hypothetical risk of identification” test proposed for the definition of “de-identified” to apply to the definition of “identifiable”, to remove ambiguity around what does and doesn’t constitute de-identified data.

**Recommendation 7**
Remove proposal 2.6 which would have a detrimental impact on research.

## Sensitive information

In addition to inferring or generating personal information from other data, it is also possible to use data as a proxy for sensitive information, for example, by using transactional data, web browsing data, or location data, to infer an individual’s sexuality, religion, union membership or political affiliation. This can be achieved without use of any sophisticated predictive analytics or machine learning technology. As highlighted above, the harm that may arise from mishandling an individual’s sensitive information does not diminish if that information was inferred from other information, rather than collected directly. If anything, it actually increases the possible harm, as the individual in question is less likely to be aware of the collection and use of their sensitive information in such contexts.

**Recommendation 8**
Ensure the definition of “sensitive information” aligns with the new definition of personal information, including a change from "about" to "relates to", as well as inclusion of information that is generated, inferred, or can otherwise act as a proxy for sensitive information. Consider introducing a “reasonable suspicion” test such that if an entity could or should have had a reasonable suspicion that certain personal information could be used as a proxy for sensitive information, it should be treated as sensitive information under the Privacy Act.

## Notice and Consent

The notice and consent model has received a significant amount of criticism over the past two decades as a result of the increased sophistication and ubiquity of digital technologies. The notion of "consent fatigue" arose to describe the experience of individuals being

bombarded with collection notices and requests to provide consent for data collection while using online services, while not being able to meaningfully engage with the process.

The notice and consent model is based upon the notion of information exchanges occurring as a translation, usually at a single point of collection or defined moment where an individual hands over their personal information. This is even reflected in APP 5.1 which requires that at the time of collection, or as soon as practicable after, steps must be taken to notify an individual.[15] This may continue to be the case when signing up for a service, or filling out a form, but it does not adequately grapple with the reality that the vast majority of data collection occurs "behind the scenes", or that much data collection is continuous and ongoing, rather than something that happens at a single point in time.

Collection notices—among other forms of privacy communications including terms of service and privacy policies—are well understood to be an ineffective means of communication for the majority of individuals. A 2020 study found 74% of participants completely skip reading any of the privacy communications for social media services. Even those who did read them did not do so carefully or were not able to understand the implications, with 98% of the participants missing "gotcha clauses" about data sharing with the United States National Security Agency, their employers, or about providing a first-born child as payment.[16]

Notice is, in theory, an important contributor to transparency. However, given that so few individuals understand lengthy and complex privacy communications, the current use of collection notices can actually undermine rather than enhance genuine transparency. DRW supports the intention of proposals **8.1** - **8.4** to clarify, standardise, and streamline requirements for collection notices and privacy policies. However, we have expressed our concern regarding the development of the OP Code in our submission to the Online Privacy Bill, which we reiterate here with reference to proposal **8.3**.[17]

While standardising the way that privacy is communicated to individuals is a welcome step, it only goes part of the way to creating meaningful control of personal information for individuals. An additional aspect of standardisation that would offer individuals increased agency would be a requirement to offer a standardised ability for individuals to opt out of *all* personal information that is unnecessary to the technical functionality of a service. This could include, for example, a requirement to offer an easy, clear, one click method to opt out of any non-essential cookies, rather than having to navigate ambiguous preference settings.

We do note that one of the ongoing issues in Australia is that organisations continue to confuse the difference between a privacy policy, collection notice, and consent. We have observed many organisations asking individuals to consent to privacy policies, or providing a

---

[15] The Privacy Act, sch 1, APP 5.

[16] Jonathan A. Obar, and Anne Oeldorf-Hirsc, 'The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services,' Information, Communication & Society 23, no. 1 (2020).

[17] Submission to the Attorney-General on the proposed Online Privacy Bill, *Digital Rights Watch,* December 2021. Available at: https://digitalrightswatch.org.au/2021/12/07/submission-online-privacy-bill/

privacy policy-like document where a collection notice ought to be. Such confusion contributes to the unreasonable challenge placed upon individuals seeking to understand and exercise meaningful control over their privacy. We strongly encourage any reforms to collection notices, privacy policies, and consent mechanisms to take into consideration how to make these forms of communication more clearly distinct, to minimise confusion for both organisations and individuals, and to minimise the occurrence of unnecessary reliance upon consent where another lawful ground for collection is present.

Consent is a key concept within privacy and information self-determination for individuals. However, it should not be able to be manipulated by entities seeking to "just get consent" as a green light to do whatever they choose with that information. It also should not be used as the default mechanism to establish legal grounds to collect, use, or disclose personal information, as is currently too often the case. The current norm of seeking consent where it is not required (be it out of misunderstanding, laziness, or due to a risk averse culture of organisations) has played a role in consent fatigue, and has contributed to diminishing the weight and meaning of providing consent.

As such, DRW supports proposal **9.1** to strengthen the definition of consent. We would also like to see further clarification that consent cannot be considered to be ongoing, specifically to ensure that entities cannot rely on consent that has since been withdrawn. We also wish to highlight that the notion of consent would benefit from an assurance that deceptive or manipulative practices, such as those the use of "dark patterns" do not constitute valid consent.

**Recommendation 9**
Strengthen the meaning of consent as in proposal 9.1. We further suggest that the definition of consent should also clarify that consent is not permanent or ongoing, and can be withdrawn.

**Recommendation 10**
Consent shouldn’t be used as a way to circumvent complying with purpose limitation and other limits and protections. For consent to be meaningful, it needs to be provided as a result of a genuine choice that is made from a position of knowledge. It must not become a transactional, box ticking requirement, that then serves as a licence to use personal information without limit.

**Recommendation 11**
Include standard requirements to allow people to opt out of all collection of information that is not essential to the technical functionality of a service.

## Additional protections for collection, use, and disclosure of personal information

We support the intention in the *Discussion Paper* to reduce reliance on the "notice and consent" model, which has proved to be an ineffective self-management approach to privacy

regulation. While notice remains an important factor for transparency, and consent is indeed essential to autonomy and self determination, they are not enough.

Organisations should not be able to use consent as go-to mechanism to green-light whichever data practices they wish to pursue, nor should they be able to bury the details in privacy communications and call it "transparency". For too long entities in Australia have been able to *technically* comply with privacy law by obtaining consent, all the while still pursuing harmful data practices and sidestepping meaningful or genuine respect for, or protections of, information privacy.

Regulated entities should be required to handle personal information in a fair and reasonable manner, rather than relying on notice and consent mechanisms to be able to place the responsibility upon individuals under the illusion of choice. Victorian Information Commissioner Sven Blummel said: “we don’t get asked for consent to walk into a dangerous building—we’re simply not allowed… we expect standards and processes to be in place to ensure they’re safe”.[18]

As such, DRW is pleased to see a recognition in the *Discussion Paper* that Australia needs a more holistic approach to privacy protections, by way of proposals **10.1 - 10.4** in which organisations can only collect, use, and disclose personal information when it is fair and reasonable to do so.

DRW are concerned that the current scope of the “fair and reasonable” test allows for too much room for companies to argue that privacy-invasive practices, or practices which cause downstream privacy harms, are still "fair and reasonable" because it is "reasonably necessary to achieve the functions and activities of the entity" or the "loss of privacy is proportionate to the benefits".[19] Given that many digital platforms base their value on the notion of an exchange of a free service in return for data extraction, it is not a challenge to imagine such a company arguing that their privacy-invasive practices are "fair and reasonable". **It is critical that there be a legislative limit placed on data centric business models to avoid companies and governments relying on their dependence on this as a fair and reasonable basis for collection and use of personal information.**

The GDPR’s legitimate interest basis for processing personal data is a useful point of comparison here. Under Article 6 of the GDPR there are six lawful bases for processing data, one of which is "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party" which is similar to point 4 of the proposed legislated factors under proposal **10.2**. However, this lawful basis goes on to add: "except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject".[20] Given that there is no federally enshrined right to privacy in Australia,

---

[18] See: ‘To consent and beyond,’ 2020, *Office of the Victorian Information Commissioner*. Available at: https://ovic.vic.gov.au/blog/to-consent-and-beyond-are-no-go-zones-the-next-frontier-part-2/

[19] Dot points 4 and 5 under proposal 10.2 of the Privacy Act Review Discussion Paper, which lists legislated factors relevant to whether a collection, use, or disclosure of personal information is fair and reasonable in the circumstances.

[20] GDPR, Article 6. Available at: https://gdpr-info.eu/art-6-gdpr/

balancing the functions or activities of an entity against rights and freedoms does not work in this context in the same way as it does in the GDPR. This exemplifies one of the limitations presented to reforming the Privacy Act without also creating a federal right to privacy. With a federal right to privacy, tests such as the "fair and reasonable" one would be able to include a much needed rights-based consideration.

**Recommendation 12**
Refine the list of legislated factors under proposal 10.2 to narrow the scope of what might be disingenuously argued to be "fair and reasonable". We suggest that this may include considering a hierarchy or weighting of legislated factors, for instance, that business interests should always be weighted far less than the best interests of a child.

**Recommendation 13**
Clarify further that the fair and reasonable test is a *threshold* test, and that if that test for an activity is failed, entities cannot use another ground for the practice.

**Recommendation 14**
Introduce a qualifier to point 4 of the legislated factors under proposal 10.2, so that the “fair and reasonable” test requires the functions and activities of an entity are balanced with how those practices impact or undermine the fundamental rights and freedoms, autonomy, or interests of an individual.

**Recommendation 15**
The OAIC should offer guidance regarding how to satisfy the fair and reasonable test in practice, including examples of practices that would *not* be considered fair and reasonable. This would allow some flexibility to adapt the test to the evolving nature of digital technologies.

## Restricted and prohibited acts and practices

Proposal **11.1** suggests the creation of a list of practices that would be either prohibited or else require additional protections. Of the two options presented, we **strongly prefer Option 1, which places the responsibility upon the entity** performing the restricted practice to take additional steps to protect individuals’ privacy and perform additional organisational transparency and accountability measures.

We **do not support Option 2.** As highlighted above under "notice and consent" and "additional protections for collection, use, and disclosure of personal information", emphasis should be placed on the responsibility of regulated entities to handle personal information in a privacy-enhancing way, rather than establishing a system in which individuals are compelled to "consent" to harmful practices. The burden of additional responsibility should be placed upon the organisation seeking to perform high-risk activities, *not* upon individuals.

We echo some of the concerns regarding the risk of a "compliance mentality" should Privacy Impact Assessments (PIAs) be made mandatory for restricted practices.[21] We nonetheless suggest that requiring organisations to perform a PIA for high-risk activities is not an unreasonable burden, and can act as an important due diligence mechanism. PIAs are also important documents for privacy and security researchers and civil society organisations such as DRW to access, in order to be able to hold organisations accountable. They also offer additional documentation to support investigations performed by the OAIC.

In addition to conducting PIAs for restricted practices, consideration should be given to creating a process whereby if the entity proposes a restricted activity, it must submit why it is in the interests of the individual to the OAIC, alongside the PIA. This could be conducted in a similar way to an ethics approval in tertiary education settings. Additional funding for the OAIC would be required to support such a process.

With regard to which practices should be classified as restricted, DRW appreciates the list of proposed restricted practices under proposal 11.1. While this list is a commendable start, we believe that the list could go further and benefit from additional clarification. To that end, we wish to extend our support to the list of restricted practices proposed by Salinger Privacy in which they've sought to combine high-risk or "high privacy impact" factors from Australia, Europe and the UK.[22]

Another option could be to generate a list by reference to harmful industries, which is an approach that has been adopted with respect to the regulation of broadcast advertising, for example. One approach could be that information collected by or transferred to businesses operating in harmful industries (such as alcohol, junk food or gambling for example) be subjected to restrictions or prohibitions that do not apply elsewhere. In such instances, the OAIC or similar entity could be empowered to amend and develop the list of restricted practices as technology develops and new areas of concern are identified.

DRW supports the prohibition of a small number of practices, in a similar vein to the 'no-go zones' established in Canada. We do suggest, however, that the inclusion of an additional safeguard whereby the OAIC has the power to provide special permission for prohibited practices, in the rare instance that the practice is unequivocally in the public interest. We suggest this in acknowledgement that technologies evolve and it is possible that there are future public interest uses of technologies that are currently being used in ways that are unreasonably harmful.

---

[21] Privacy Act Review Discussion Paper, page 95.

[22] Submission in response to the Privacy Act Review - Discussion Paper, 3 January 2022, *Salinger Privacy,* page 27. Available at: https://www.salingerprivacy.com.au/wp-content/uploads/2022/01/22-01-03_Privacy-Act-review_Salinger-Privacy_Submission.pdf

For example, the use of one-to-many facial recognition technology has been widely condemned by human rights organisations around the world.[23] Given the impact upon individuals right to privacy, as well as overarching negative societal impacts, DRW strongly recommends that the use of one-to-many facial recognition be included as a prohibited practice.

**Recommendation 16**
We support the introduction of restricted practices. Such activities should trigger a requirement for APP entities to implement additional protections and organisational accountability measures (Option 1 under 11.1), rather than relying on an individual privacy self-management approach (Option 2).

**Recommendation 17**
A small number of prohibited practices should be introduced which represent unreasonable risk of harm and undue interference with privacy. We recommend that one-to-many facial recognition be included in this list.

## Children and vulnerable individuals

The question of how best to uphold the privacy of children has received an enormous amount of attention over the past several years. We wish to emphasise that while we agree that children and vulnerable individuals are indeed at greater risk of harm as a result of their personal information being handled inappropriately, that robust privacy protections for *everyone,* including the creation of a federal right to privacy, would go a long way to protect those children and vulnerable people.

Proposal **13.1** presents two options for implementing parental or guardian consent where a child is under the age of sixteen. Option 1 requires parental or guardian consent to be required before collecting, using, or disclosing personal information of the child under the age of sixteen in all instances. Given the nature and core functionality of digital services, such an approach is not practicable. Consent is not required for many instances of collection, use, and disclosure currently under the Privacy Act. Introducing this requirement is counterintuitive to the notion that reliance upon consent should be minimised, in order to ensure it remains meaningful (see earlier discussions under "notice and consent" and "additional protections for the collection, use, and disclosure of personal information"). Further, there are many legitimate and routine activities in a child's life that require personal information that should not require a parent or guardian's consent in every instance. In fact, requiring a parent or guardian to provide consent for routine and lawful activities may result in halting some activities which could in turn work against the best interests of the child. Given these significant impracticalities, **we do not support Option 1 under proposal 13.1.**

[23] For further detail regarding the risks of one-to-many facial recognition, see 'Human Rights and Technology' Final report, 2021, *Australian Human Rights Commission.* Available at: https://tech.humanrights.gov.au/

DRW has previously commented on some of the other possible issues related to reliance on parent and guardian consent, as well as the challenges of affording children increased protections by way of age verification or assurance mechanisms, in our previous submission on the Online Privacy Bill, which we wish to reiterate here.[24]

Finally, we are concerned that the intention behind proposal **13.1** falls into the same trap that the current iteration of the Privacy Act has: **an overreliance on an individual responsibility framework of privacy self-management, as opposed to robust regulation of the practices and activities of the organisations handling the personal information.**

While relying on consent to handle personal information that relates to children is an imperfect solution to minimise privacy harms to children, there is a need for additional protections regarding how the personal information of children is collected, used and disclosed. To that end, we submit that entities that handle personal information relating to children, or that design products or services which are reasonably expected to be used by people under the age of 18, should be subject to additional obligations to ensure their practices do not cause undue privacy-related harm, especially to children.

We note, however, that efforts to afford children additional privacy protections should not come to realisation via implementation of mechanisms that rely on additional surveillance or privacy-invasive practices. For example, the requirement to use age verification as proposed under the draft Online Privacy Bill.[25] Instead, DRW would prefer to see entities who reasonably expect to handle personal information that relates to children embed robust privacy-enhancing practices across the board, rather than attempting to differentiate individuals, and thus the protections afforded to them, based on age.

**Recommendation 18**
Entities that handle personal information relating to children should be subject to additional obligations to embed additional privacy protections, such as restricting secondary use of personal information of children.

---

[24] Submission to the Attorney-General on the proposed Online Privacy Bill, *Digital Rights Watch,* December 2021. Available at: https://digitalrightswatch.org.au/2021/12/07/submission-online-privacy-bill/

[25] For further detail on why age-verification is privacy-invasive, refer to the submissions that Digital Rights Watch made to the eSafety Commission on the draft Restricted Access System (RAS) Declaration, 23 November 2021, available at: https://digitalrightswatch.org.au/2021/11/25/submission-draft-restricted-access-systems-declaration/ And the submission to the Attorney-General on the proposed Online Privacy Bill, *Digital Rights Watch,* December 2021. Available at: https://digitalrightswatch.org.au/2021/12/07/submission-online-privacy-bill/

## Exemptions

DRW was disappointed to note that the *Discussion Paper* did not include any specific proposals to remove the exemptions for small businesses, employee records, political parties, and media organisations. We examine each in turn below.

### Small business exemption

The privacy protections offered to individuals should not be subject to the size of the organisation that is handling their personal information. The small business exemption does not reflect the possible privacy harms that can arise from small businesses' use of personal information, especially given the widespread availability and use of affordable third party platforms and services enabling small business to collect, use, store, and disclose personal information in ways that may not have been available to them 20 years ago, when the exemption was first introduced.

Over the course of the COVID-19 pandemic, small businesses throughout Australia have been required to collect personal information for public health purposes. We have heard significant concern from community members regarding the privacy and security of that information, and an unease that these businesses were neither equipped nor required to protect the information that they collected.

We appreciate that removing the small business exemption may create a compliance and administrative burden upon small businesses. However, we also would highlight that the flexible nature of the APPs already allows for small businesses to apply measures commensurate to their position, circumstances and risk profile, according to the inclusion of "reasonable steps" in many of the principles.

Privacy is a human right, and the need for digital security is not going to diminish. The small business exemption is a prime example of how privacy in Australia is considered under a value-based rather than rights-based framework. In order to participate in the digital economy in a responsible manner, small businesses need to play their role in protecting the privacy and security of people's personal information. Further, the *Discussion Paper* notes that "no comparable jurisdiction exempts small businesses from the general privacy law." It is time for Australian privacy law to catch up with our international counterparts, and in turn, be able to participate more actively in the global economy.

**Recommendation 19**

The Privacy Act must apply to any and all entities which collect, process, or otherwise handle personal information. The flexibility of the APPs already allow regulated entities to take a risk-based approach based on their particular circumstances, including size, resources, and business model. Therefore the compliance costs would be commensurate with their risk profile.

**Recommendation 20**
Provide small businesses with additional, targeted resources and support to adopt the privacy practices required by the Privacy Act. Additional funding to the OAIC or another entity should be provided to make this possible.

## Political exemption

It is unacceptable for registered political parties to continue to be exempt from the Privacy Act. Organisations and businesses should not be subject to one set of rules, while political parties get free reign. If political parties are unable to conduct their political messaging and outreach without utilising practices that are not permissible to other entities under the Privacy Act, then that is a clear indication that those practices should not be acceptable.

While some argue that this exemption is important for freedom of political communication, we argue that it actually poses a risk to the democratic process. The increased sophistication of targeted marketing, including hyper-personalisation, presents a real and significant risk of voter manipulation, which in turn would undermine people's ability to participate freely in democracy. We support and echo the concerns highlighted in the *Discussion Paper* with reference to Cambridge Analytica as a prime example as to why the political exemption is not appropriate.[26]

We further note that there is public support for removal of this exemption. A survey of 1606 Australians in 2021 found that 80% are in favour of making political parties subject to the full Privacy Act, and only 5% are against.[27] Similarly, the OAIC's 2020 Community Attitudes to Privacy Survey revealed that 74% of respondents believe political parties should be subject to the Privacy Act.[28]

**Recommendation 21**
Remove the political exemption as a part of reviewing the Privacy Act.

---

[26] As we have seen through reports and documentaries such as *The Great Hack*, the exemption for political messaging poses a unique threat to our democracies. Over the last decade we have seen an explosion in the practice of profiling and targeting individuals for political messaging. Personalised news feeds, ads and other individual-targeted content online can more easily facilitate misinformation than offline political advertising could achieve. As a result, the risks posed to the privacy of individuals, the stability of our democratic government, and public trust in public institutions have exponentially increased.

[27] 'Voters want to ban politicians from spamming them with texts and calls,' September 2021, *The Sydney Morning Herald.* Available at: https://www.smh.com.au/politics/federal/voters-want-to-ban-politicians-from-spamming-them-with-texts-and-calls-20210924-p58uko.html

[28] OAIC, *Australian Community Attitudes to Privacy Survey,* 2020, page 60. Available at: https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page

## Employee records

All individuals should be afforded the right to privacy and appropriate protection of their personal information, including while working.

The employment relationship necessitates the collection of an immense amount of personal, and often sensitive, information. This, combined with the power imbalance in the employee-employer relationship, creates a dynamic in which employees have very little choice but to provide whatever information their employer requests. That information should enjoy the protections offered by the Privacy Act.

We do note, however, that there is some difficulty in extending the Privacy Act to include employee records, in that even by doing so it does not get to the heart of the problem, as privacy issues in the workplace are complex and not limited to how records are handled. For example, social media monitoring of employees, surveillance in non-work areas such as break rooms, “checking into” shifts via an app that uses facial recognition or other biometric software are all examples of privacy issues in the workplace that would not be easily solved by removing the employee records exemption.

Further, the nature of work and the employment relationship is evolving, and the boundaries between work and private life are diminishing. Many employees use their own devices for work purposes, mixing their personal information with work data. Many employers are also implementing increasingly invasive productivity measurement technologies and workplace surveillance measures. This has been exacerbated by the COVID-19 pandemic, which has resulted in many employees working outside of their usual business environments, and the use of these technologies thereby expanding into people’s private residences.

Given the inequalities inherent in most employer-employee dynamics, amplified by the increasingly invasive surveillance technologies available to employers and deployed outside of traditional workplace environments, it is absurd that employers are not required to comply with the security requirements of APP 11.1, that would otherwise require them to protect the personal information of their employees from misuse, interference, loss, unauthorised access, modification, and disclosure.

The Privacy Act was not designed with the workplace in mind, and in the face of changing working conditions and expectations is likely to be even less fit-for-purpose in modern, technological employment relationships. Workplace privacy concerns are complex, so simply applying the Privacy Act to the workplace is unlikely to get to the core of the issue. To that end, DRW strongly suggests that further investigation is undertaken in this area.

**Recommendation 22**
Remove the employee records exemption, or, commit to standalone workplace surveillance legislation.

**Recommendation 23**
Further investigate existing workplace surveillance practices across Australia to identify what is needed to adequately protect workers' rights; balancing digital privacy of workers with reasonable monitoring requirements within an employment relationship, and the ongoing impacts of the COVID-19 pandemic with regard to the extension of workplace monitoring into personal environments.

### Journalism exemption

There is a genuine and important need to balance the public interest in privacy protection with a free and robust press. DRW supports the need for special treatment of public interest journalism activities. However, we also note that there are examples of unreasonable invasions of privacy by the media which served no genuine public interest or investigative value, such as doxxing and public shaming of people breaching local pandemic regulations. [29] There is an important distinction between "in the public interest" and "what the public might be interested in".

We also support the proposal to extend the data security requirements of APP 11 to media organisations, which would require them to take reasonable steps to protect the personal information they hold from misuse, interference, loss, unauthorised access, modification, or disclosure. This application of APP 11 to media organisations would not prevent them from their journalism activities, but it would reflect the genuine need to instil good digital security practices to protect the personal information they hold. It would also require them to dispose of personal information they are no longer using, which is a reasonable expectation and an important measure to decrease the risk of data breach or other privacy harms to individuals in the future.

**Recommendation 24**
Introduce a public interest test to the journalism exemption, such that it will only apply where journalism is in the public interest. The public interest test should include consideration of the rights of the individual.

**Recommendation 25**
Extend the application of APP 11 on data security to media organisations.

## Direct right of action

Australia should consider adopting a rights-based approach to the issue of privacy. In a data-driven economy, the rights of individuals should be the foundation of this review, and ensuring that Australians have direct rights of action when their privacy is violated or their personal information mistreated is essential in holding internet platforms, advertisers, and malicious parties to account.

[29] See, for example: https://twitter.com/StefArmbruster/status/1433194476114087938

The rights granted under the EU GDPR should be a starting point for developing a similar rights-based system for the Australian context. While some rights, such as "the right to portability" already exist in Australia, there are other vital rights under the GDPR such as the "right to explanation", "right to rectification", and "right to erasure".[30] Specifically, the "right to explanation" is critical in helping individuals understand how their personal information was used in making decisions, creating accountability between individuals and the entity processing their information. This matter has been considered by the Australian Human Rights Commission in their discussion paper on Human Rights and Technology.[31]

**Recommendation 26**
Breaches of the APPs should give individuals the right to bring a case in court (not just to the OAIC), including as representatives of a class. For such cases, there should be a regime of civil penalties for breaches of the APPs that can be awarded to the individual.

## Automated decision-making

We note that there is consideration of automated decision making within the *Discussion Paper,* but that there is no suggestion or proposal of any new rights in this space or meaningful changes to improve privacy with regard to automated decision making.

The use of Artificial Intelligence (AI), and other forms of automated decision-making is receiving increasing attention and regulation around the world. The GDPR includes a right to "meaningful information about the logic involved" in automated decisions, as well as a requirement for "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests".[32] [33] The European Commission is considering an AI-specific law, as are several states in the United States.[34] [35]

We do not believe that **17.1** will have any meaningful impact or reduction of the possible harms caused by automated-decision making systems. Including information as to whether a person's personal information will be used in an automated decision making system is the absolute bare minimum that organisations should be required to meet.

---

[30] We recognise that the "right to erasure" has been misinterpreted globally and applied in very different ways across the EU member states. We would encourage the AG to consider the best practices for the Australian context. More in Access Now's paper on the Rights to be Forgotten globally. Available at: https://www.accessnow.org/cms/assets/uploads/2017/09/RTBF_Sep_2016.pdf
[31] 'Human Rights and Technology' Final report, 2021, *Australian Human Rights Commission.* Available at: https://tech.humanrights.gov.au/
[32] GDPR, Articles 13-15
[33] GDPR, Article 22
[34] Proposal for harmonised rules on artificial intelligence, European Commission. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206
[35] For example, see 'Legislation related to artificial intelligence,' *National Conference of State Legislatures,* January 2022. Available at: https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx

There is plenty of research to suggest that individuals do not read, nor necessarily comprehend privacy policies, so the assumption that requiring privacy policies to include information about whether a person's information will be used in automated decision-making would constitute a meaningful awareness-raising exercise is misguided. Further, without an opportunity to object to, question, or appeal decisions made by fully- or partially-automated processes, merely informing individuals of the fact that automated decision-making is happening does very little to equip individuals with the ability to seek redress where harms arise, or push for meaningful change in how personal information is used as inputs into automated decision making systems. Such an approach falls into the trap of the transparency fallacy.

**Recommendation 27**

Further consideration ought to be given to the development of provisions which give individuals a meaningful and accessible pathway to seek an explanation, audit, and review of decisions made by automated means. This should also include attribution of the automated decision to the entity that used the automated system, and compensation for any harm caused by an incorrect decision made by automated means.

---

## Contact

**Lucie Krahulcova** | Executive Director | Digital Rights Watch | lucie@digitalrightswatch.org.au
**Samantha Floreani** | Programme Lead | Digital Rights Watch | samantha@digitalrightswatch.org.au