Submission to the Attorney-General's Department on the 2022 Report regarding the review of the *Privacy Act 1988*

31 March 2023

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.[1]

[1] Learn more about our work on our website: https://digitalrightswatch.org.au/

Overview

We welcome the opportunity to submit comments to the Attorney-General's department concerning the 2022 Report of the review of the Privacy Act 1988 (the Report). Digital Rights Watch (DRW) has been actively participating in the consultation process throughout the review of the Privacy Act since it commenced in 2020. In addition to our formal submissions, we have hosted a range of community events and roundtables to better understand the needs and expectations of other advocacy and interest groups, as well as the community more broadly.

Our previous submissions regarding the Privacy Act can be found here:

- Privacy Act Review - Issues Paper, November 2020[2]
- Privacy Act Review - Discussion Paper, January 2022[3]
- Proposed Online Privacy Bill, December 2021[4]
- Senate inquiry into the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022,* November 2022[5]

In addition to this, DRW regularly participates in public debate and consultation processes regarding the development and implementation of other law and policy that stands to impact the right to privacy in Australia. Relevant submissions include:

- Data Availability and Transparency Bill, November 2020[6]
- Electronic Surveillance Reform Discussion Paper, February 2022[7]
- Online Safety - Restricted Access Systems and Age Verification, November 2021[8]

---

[2] Digital Rights Watch submission to the Attorney-General on the Issues Paper regarding the review of the *Privacy Act 1988,* November 2020.
https://digitalrightswatch.org.au/2020/11/27/submission-privacy-act-review-issues-paper/

[3] Digital Rights Watch submission to the Attorney-General's Department on the Discussion Paper regarding the review of the *Privacy Act 1988,* January 2022.
https://digitalrightswatch.org.au/wp-content/uploads/2022/01/Submission_-Privacy-Act-Review-January-2022.pdf

[4] Digital Rights Watch submission to the Attorney-General's Department on the proposed *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021,* December 2021.
https://digitalrightswatch.org.au/2021/12/07/submission-online-privacy-bill/

[5] Digital Rights Watch submission to the Senate Standing Committee on Legal and Constitutional Affairs regarding the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022,* November 2022.
https://digitalrightswatch.org.au/wp-content/uploads/2022/11/DRW-Submission-Privacy-Legislation-Amendment-Bill.pdf

[6] Digital Rights Watch submission to the Office of the National Data Commissioner on the proposed Data Availability and Transparency Bill 2020, November 2020.
https://digitalrightswatch.org.au/2020/11/12/submission-the-data-availability-and-transparency-bill/

[7] Digital Rights Watch submission to the Department of Home Affairs in response to the 'Reform of Australia's electronic surveillance framework' Discussion Paper, February 2022.
https://digitalrightswatch.org.au/wp-content/uploads/2022/02/Digital-Rights-Watch-submission-to-the-surveillance-review-discussion-paper-February-2022.pdf

[8] Digital Rights Watch submission to the Office of the eSafety Commissioner on the draft Restrcted Access Systems Declaration 2021, and the roadmap for age verification for online pornography, November 2021.
https://digitalrightswatch.org.au/wp-content/uploads/2021/11/Submission_-Draft-Restricted-Access-System-Declaration-eSafety-Commissioner-November-2021.pdf

General remarks

Privacy is essential to upholding democracy, reining in corporate power, and for a safe and fair digital future.

The Privacy Act must not only enhance individuals' ability to exercise their rights and enhance their autonomy, agency and dignity in the digital age. It must also fundamentally challenge the harmful business models of data generation, extraction, and commodification commonly referred to as 'surveillance capitalism'.

While reading the Report, we were concerned to note how often privacy was regarded as secondary to commercial interests. The insistence that protecting privacy should not disrupt the business practices of some of the worst players in the digital age, such as data brokers, is disturbing. The data practices of many of these companies are dangerous, and *ought to be challenged*. Privacy has a critically important role to play in addressing the problems created by surveillance capitalism because it strikes at the heart of harmful business models that extract and exploit our data. We urge the Attorney-General's Department not to shy away from bold privacy reform which puts businesses operating under a surveillance capitalism logic on notice.

A bold agenda for privacy reform in Australia can not wait any longer. The Optus and Medibank breaches of 2022 revealed to millions of people just how dangerous it can be to collect too much personal information and store it for far too long. The recent Latitude Financial breach has further highlighted this, with 14 million people impacted—some of whose information was collected up to 10 years ago. This is unacceptable and the Australian government must prioritise privacy and security reform as a matter of urgency.

At the heart of privacy reform must be a prioritisation of data minimisation. We know that perfect data security doesn't exist, so the best way to keep personal information safe is not to have it. There is currently a pervasive culture of data-hoarding in which organisations collect and store far too much information "just in case" it may be useful or profitable in the future. We need the Privacy Act to challenge this culture by placing stricter limits on collection, use and disclosure of personal information, as well as stronger requirements to ensure it is not retained any longer than necessary.

We note that there has been a lot of attention in the report directed toward targeted advertising and direct marketing. While these practices do indeed deserve scrutiny, they are but one of the outcomes of surveillance capitalism. For instance, personalised content curation and recommender systems on digital platforms — sometimes referred to as algorithmic 'rabbit holes' — use a lot of the

same logic as targeted advertising and personalisation, and result in some incredibly alarming online harms such as exposing young people to increasingly troubling eating disorder or self harm content on TikTok. Such rabbit holes also contribute to political polarisation and incentivise the creation and spread of disinformation.

What's more, companies are buying and selling personal information to accumulate wealth and serve their corporate interests. The shadowy data broker industry doesn't just lead to a commercialised online experience, it also materially impacts people's choices, opportunities and access to services in sectors like education, healthcare, finance, insurance and housing. This can occur in a number of ways, including the increasing use of automated decision making or machine learning systems which use personal information as inputs.

Protecting privacy and pushing back on surveillance capitalism is about so much more than just targeted advertising and minimising the harms of data breaches.

In considering the proposals contained in the report, DRW focused our attention to a set of criteria that we believe a reformed Privacy Act should prioritise. A reformed Privacy Act must:

- Expand the rights and agency of individuals over their personal information.
- Challenge the business models of data-extractive companies and rein in corporate power including, but not limited to Big Tech.
- Support democracy in the digital age.
- Require the responsible, fair, and reasonable use of data in the public good, and place responsibility upon organisations rather than just individuals.
- Increase transparency of data practices and enhance accountability of organisations handling personal information.
- Reduce the reach of surveillance in people's everyday lives by minimising the amount of personal information collected, stored, used, and shared.

As this is the third round of consultation for this review, we have kept our feedback relatively high-level. We welcome the opportunity to provide in-depth comments in response to draft legislation. For the purpose of this submission we have addressed the following key areas:

1. Personal information and de-identification
2. The fair and reasonable test
3. Consent
4. Exemptions to the Act
5. Direct right of action and a statutory tort for serious invasions of privacy
6. Rights of the individual
7. Direct marketing, targeting, and trading of data
8. Children's privacy

Summary of recommendations

1. Implement proposals 4.1 and 4.3 to ensure that the definition of personal information includes both technical data as well as information that is inferred or generated.

2. Amend proposal 4.4 to ensure that an individual is 'reasonably identifiable' if they are capable of being distinguished from all others, even if their identity is not known.

3. Implement proposal 4.5 to amend the definition of 'de-identified', however further amendments through the Privacy Act will need to be made to accommodate the new, weaker definition. For example, de-identification cannot be considered to be equivalent to deletion.

4. Do not implement proposal 4.7 to further consult on the introduction of introducing a criminal offence for malicious re-identification of de-identified information.

5. Implement proposal 12.1 to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances.

6. Ensure the fair and reasonable test applies regardless of whether consent has been obtained, however proposal 12.3 should be amended to apply to all instances—including those authorised under APPs 3.4 and 6.2.

7. Clarify the factors to be considered in determination of "fair and reasonable" to ensure that entities cannot justify privacy-invasive practices because they are "reasonably necessary for the functions and activities of the organisation."

8. Ensure the fair and reasonable test prioritises safety. Implement a 'best interests' framework as part of the fair and reasonable test, extending the framework to apply to all people, not just children.

9. Define consent as voluntary, informed, current, specific, and an unambiguous indication though clear action.

10. Abolish the small business exemption, the political party exemption, and the employee records exemptions. Introduce limited exceptions to relevant APPs where necessary.

11. Adopt the proposed updates to the journalism exemption.

12. Allow complainants the choice as to whether to file a complaint first with OAIC (before a court action can commence) or directly to a court.

13. Implement both a direct right of action and a statutory tort for serious invasion of privacy.

14. Introduce a power to award civil penalties to individuals who have experienced an interference with their privacy as part of a direct right of action.

15. Implement the range of new or expanded individual rights, ensuring that organisations cannot avoid meeting the requirements by leveraging or manipulating the meaning of “reasonable steps”.

16. Any direct marketing or targeted advertising should be opt in.Ensure that consent cannot be forced by way of tying it to the provision of goods and services.

17. Amend proposal 20.4 to prohibit the trade in personal information.

18. Do not require or incentivise the implementation of age verification.

Personal information and de-identification

The updated definition of 'personal information' must discourage surveillance and challenges the business models of data extraction and targeted advertising.

'Personal information' should include technical data (such as metadata), inferred or generated data (for instance, when Facebook or TikTok can predict your political beliefs or sexuality from your behaviour), and other techniques that can distinguish individuals from a group—because privacy related harms can occur even if the organisation doesn't know your name. To that end, we welcome proposals 4.1 and 4.3.

We remain concerned, however, that there is confusion in the Report regarding 'reasonably identifiable' with regard to indirect identification, 'individuation', or the ability to single out or distinguish an individual from a group.

We note the Discussion Paper stated 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".[9] However, we are concerned to see that this intention appears to have been walked back in the Report. As privacy Law expert, Anna Johnston, has emphasised: rapid advances in technologies, including artificial intelligence and facial recognition, and business practices involving probabilistic and other forms of data linkage, mean that 'not identifiable by name' is no longer an effective proxy for 'will suffer no privacy harm'.[10]

There is a broad range of negative consequences that can arise as a result of being able to single out individuals, regardless of whether that coincides with knowing their personal identity or not. This is not limited to targeted advertising or targeting based on online behavioural data—although these use cases certainly warrant attention. The ability to distinguish individuals from a group also fuels the data broker industry in which data is bought, sold and speculated upon; contributes to the impact of machine learning models or algorithmic decision making systems; enhances the spread of mis- and dis-information, as well as detrimental content curation algorithms or recommender systems (also known as algorithmic 'rabbit holes').

If Australia is serious about seeking to challenge the harmful practices of dominant social media apps and digital platforms more broadly, then we must include individuals being distinguished from all others, even if their identity is unknown, in the explanation of "reasonably identifiable."

---

[9] Privacy Act Review Discussion Paper, page 27.

[10] Anna Johnston, 2020, "Individuation: Re-imagining Data Privacy Laws to Protect Against Digital Harms" (electronic). Brussels Privacy Hub. 6 (24); available at https://brusselsprivacyhub.eu/publications/wp624.html

As such, the wording of the definition of personal information under the Act must make it clear that it includes where an individual may be singled out and acted upon, even if their identity is not known. This is in line with what the OAIC considers to constitute personal information—an individual is "identifiable" where they are "distinguished from all others in a group"[11]

De-identification

We support the proposed updated definition of de-identified data in proposal 4.5, as it emphasises the limitations of de-identification. However, it is important that the subsequent proposals regarding the treatment of de-identified information be adjusted to accommodate the weaker definition. It is unreasonable in our view that the report appears to accept that most de-identified data carries a significant re-identification risk, but it nonetheless seeks to exclude such data from key protections in the Act. Among other things, if de-identified information is to be regulated as a category that is distinct from personal information, then its use and disclosure should still be subject to the fair and reasonable test and reasonable steps should be taken to ensure its data security.

We support Professor Vanessa Teague's submission, in which she notes that: "everything bad that can be done with explicitly re-identified data can be done with identifiable data too...the solution is to protect all identifiable personal data as personal information."[12]

Similarly, we support the submission of Salinger Privacy which notes that:

> *"if the definition of 'personal information' was amended to clearly state that 'an individual is "identifiable" if they can be distinguished from all others in a group' this would offer suitable protections in relation to de-identified data posing a high likelihood of re-identifiability, because reidentifiable data would be considered 'personal information', without creating a new compliance burden in relation to de-identified data posing a low or remote likelihood of reidentifiability."*[13]

Recommendations

1. Implement proposals 4.1 and 4.3 to ensure that the definition of personal information includes both technical data as well as information that is inferred or generated.

[11] Commissioner initiated investigation into Clearview AI, Inc. (Privacy) [2021] AICmr 54 (Clearview Determination); Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) AICmr 54 (7-Eleven Determination).
[12] Vanessa Teague, Submission to the Report
[13] Salinger Privacy, Submission to the Report

2. Amend proposal 4.4 to ensure that an individual is 'reasonably identifiable' if they are capable of being distinguished from all others, even if their identity is not known.

3. Implement proposal 4.5 to amend the definition of 'de-identified', however further amendments through the Privacy Act will need to be made to accommodate the new, weaker definition. For example, de-identification cannot be considered to be equivalent to deletion.

4. Do not implement proposal 4.7 to further consult on the introduction of introducing a criminal offence for malicious re-identification of de-identified information.

The fair and reasonable test

We welcome and strongly support proposal 12.1 to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. We also support that the fair and reasonable test should apply irrespective of whether consent has been obtained.

We do, however, strongly recommend that the fair and reasonable test should apply to *all* instances of collection, use and disclosure of personal information, including those authorised under APPs 3.4 and 6.2. There is no valid reason why law enforcement bodies should not also be required to collect, use and disclose personal information in a way that is fair and reasonable. In fact, given the higher likelihood of harm that may occur as a result of misuse or abuse of personal information in a law enforcement context, it is essential that these bodies be required to handle personal information in a manner that is fair and reasonable. It's also unlikely this requirement would substantially impair the ability of law enforcement bodies to carry out their activities, as law enforcement bodies are already subject to review and complaint procedures where they act contrary to community expectations and standards.

With regard to the factors in determining whether a collection, use or disclosure is fair and reasonable, we reiterate the same concern as in our submission to the Discussion Paper: that the test may allow for entities to argue that privacy-invasive practices are still "fair and reasonable" because it is "reasonably necessary to achieve the functions and activities of the organisation."[14] Given that many digital platforms' and intermediaries' entire business model is to generate, extract and commodify data (including personal information), it is not hard to imagine how such entities would argue that their privacy-invasive practices are

[14] Privacy Act Review Report 2022, p. 120. Point (c) under proposal 12.2.

"reasonably necessary to achieve the functions and activities of the organisation" and therefore "fair and reasonable."

As such, if point (c) under proposal 12.2 was the *only* factor considered by an entity, it could undermine the intention and application of this proposal. If taken alone, it can too easily be used to justify even the most invasive practices.

We recommend clarification that just because an entity has collected personal information which is reasonably necessary for a function or activity it is performing does not make the collection fair and reasonable, but an entity collecting information not related to a function or activity indicates that it has collected it in unfair or unreasonable circumstances. Point (c) is a necessary but insufficient condition to meet the fair and reasonable test.

'Reasonable' must prioritise fairness and safety

We echo the sentiments raised by Choice with regard to the need to prioritise fairness and safety for those whose data is being used and those who are impacted by any decisions made based on the data.

As such, in developing the specifics of the fair and reasonable test, we encourage the Attorney-General's Department to consider implementing a best-interests framework as part of the consideration of "reasonableness," rather than only considering best interests where it applies to children.

Recommendations

5. Implement proposal 12.1 to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances.
6. Ensure the fair and reasonable test applies regardless of whether consent has been obtained, however proposal 12.3 should be amended to apply to all instances—including those authorised under APPs 3.4 and 6.2.
7. Clarify the factors to be considered in determination of "fair and reasonable" to ensure that entities cannot justify privacy-invasive practices because they are "reasonably necessary for the functions and activities of the organisation."
8. Ensure the fair and reasonable test prioritises safety. Implement a 'best interests' framework as part of the fair and reasonable test, extending the framework to apply to all people, not just children.

Consent

Consent is an essential component of personal agency and control over personal information, but it is often treated as a tick-box exercise or a catch-all to allow dubious practices. Organisations should not be able to force, trick or manipulate people into giving consent.

DRW supports the intention to strengthen the definition of consent in the Report, however we are concerned that the Report appears to have stepped back as compared to the earlier iteration of consent as considered in the Discussion Paper. Specifically, we have concerns regarding:

1) the removal of "indication through clear action" under proposal 11.1, and
2) the ability to force consent as a condition of accessing goods or services as discussed under proposal 20.4.

In the ACCC's Final Report on the Digital Platforms Inquiry, it set out that valid consent should require a clear, affirmative act. We are concerned that should 'indication through clear action' not be implemented as part of the updated definition, it will allow for entities to continue to exploit consent as they are under the current consent requirements (which already requires consent to be voluntary, informed, current and specific).

We note that the reasoning put forward in the Report for removing the requirement for 'indication through clear action' are concerns that it would impair the ability of entities to rely on implied consent in limited circumstances (such as medical research or clinical settings). However, the effect of removing the requirement altogether is that it will allow implied consent to be relied upon in all circumstances, not just those limited circumstances contemplated by the Report where there are strong public or individual interests. Placing reliance on 'ambiguity' in the commercial setting is not sufficient as it can be difficult to determine, whereas a 'clear action' is easy to evidence.

We are also gravely concerned regarding the implications of the discussion regarding proposal 20.4 which notes that consent to trade in personal information can be tied to the provision of goods and services. Enabling companies to force consent in this way not only undermines the notion of consent being voluntary or freely given, it also stands to entrench some of the worst practices of digital platforms and loyalty schemes operating under surveillance capitalism.

Recommendations

9. Define consent as voluntary, informed, current, specific, and an unambiguous indication though clear action.

Exemptions to the Act

Domestically, the OAIC's Australian Community Attitudes to Privacy Survey 2020 found that almost three-quarters of Australians feel that each of the exempt organisation types should be required to protect personal information in the same ways that government and larger businesses are required to.[15]

We also note that the proposals contained in the Report related to the exemptions to the Act are unlikely to go far enough to result in Australia achieving 'adequacy' status in respect to the General Data Protection Regulation (GDPR). The European Commission — the body that will ultimately decide upon Australia's status — has supported the removal of all existing exemptions in the Act.[16]

Overall, our recommendation follows that of the European Commission: that the exemptions be removed, and instead, where necessary, create limited, risk-based exceptions from certain APPs (for instance, with regard to the public interest in political communication and public interest journalism).

Small Business Exemption

The Report states that it is estimated that less than 5 percent of businesses actively trading in the Australian economy had an annual turnover of more than $3 million.[17] It is unacceptable for so many companies in Australia to be able to easily collect, use, store and disclose personal information without due regard to people's privacy. People should be able to interact with Australian businesses and be confident that when they provide their personal information, it will be handled appropriately, regardless of the size of the business.

We support the removal of the small business exemption with a set grace period for compliance of no more than 12 months.

The Privacy Act is already designed to be flexible, with 'reasonable steps' able to be scaled up and down depending on a range of factors. Nonetheless, to further assist with any issues of compliance burden, the OAIC should be appropriately

[15] 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
[16] European Commission, 'Consultation on the review of the Privacy Act 1988' p. 2.
[17] Privacy Act Review Report 2022, p. 53.

resourced in order to further assist small businesses in the transition to compliance with the Privacy Act.

Political Parties Exemption

The Report notes that almost all submitters that commented on the political parties exemption considered that it was not justifiable.[18] In alignment with this, there is very clear public support for the removal of the political party exemption. A 2021 survey found that 80% believe that registered political parties should be subject to the full Privacy Act, with only 5% against.[19] This is an increase from the OAIC's 2020 Community Attitudes Survey, which showed that 74% of respondents believe political parties should be subject to the Act.[20]

The proposals 8.1 - 8.5 do not go far enough. Moreover, they place far too much responsibility upon individuals, rather than on the parties collecting and using personal information. While these proposals may increase transparency of data handling practices by registered political parties, they offer no meaningful challenge to the status quo and are unlikely to actually change existing or future data handling and privacy practices of political parties.

We reiterate our stance in previous submissions, including to the Inquiry into the 2022 Federal Election: the exemption of registered political parties from the Privacy Act enables unfair data handling practices, poses a data security risk for voters, as well as major reputational risks to the parties themselves. Bringing political parties and their associated entities under the Privacy Act is not just about managing risk. It is also an opportunity to demonstrate leadership, build trust and prove to the public that they are serious about meeting community expectations and protecting the privacy rights of voters.[21]

Rather than a sweeping exemption, we suggest that tailored public interest exceptions to APPs 3, 6, 12, and 13 be developed in order to balance political free speech with the right to privacy.

Employee Records Exemption

Everyone should be afforded appropriate protection of their personal information, including workers. Australia is one of the few jurisdictions in the world where

[18] Privacy Act Review Report 2022, p. 73.
[19] '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
[20] 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
[21] Digital Rights Watch submission to the Joint Standing Committee on Electoral Matters Inquiry into the conduct of the 2022 Federal Election, September 2022. https://digitalrightswatch.org.au/2022/09/28/submission-inquiry-into-the-2022-federal-election/

privacy protection is not afforded to employees and many jurisdictions even confer greater protection on employees, who are seen as particularly vulnerable.[22]

Whilst the raison d'etre for the exemption may have been to leave regulation up to workplace relations legislation, such legislation has not kept up with modern technology and employer practices. As echoed in our first submission, today employers are collecting a wide variety of information about employees. Without adequate regulation, this exposes employees to a variety of harm:

- Employees may feel afraid to communicate confidentiality or participate in activities because they are being monitored and surveilled.
- Employees may feel that they have to provide personal information to their employer or agree to certain uses and disclosure of their personal information - to simply keep their job.[23]
- The quantity and nature of personal information that employers keep, without a legislative stick to ensure that employers take data security safeguards, exposes employees should a data breach occur and limits their rights of recourse.[24]

We are therefore concerned that proposal 7.1 does not go far enough. A simpler and likely more effective solution would be to abolish the exemption but then to introduce limited exceptions to APP 12 (to deal with the issues raised in relation to access) and APP 13 (to deal with the issues raised in relation to correction).

As we previously discussed in our submission to the Discussion Paper, simply abolishing the employee records exemption is unlikely to address the complex and evolving issues of workplace surveillance and worker privacy. As such, we also suggest that further investigation be directed towards developing legislation to protect workers from unreasonable workplace surveillance.

Journalism Exemption

Digital Rights Watch strongly supports public interest journalism and the public value of a free and robust press. As such, we support the special treatment of public interest journalism activities to ensure that the needs of a free press are balanced with the public interest in the right to privacy.

---

[22] For example, under the GDPR, the processing of employee data in an employment context may be considered high risk and mandate a data protection impact assessment, the Art 29 Data Protection Working Party recognising that "there are increased power imbalances between the data subjects and the data controller" (see *Guidelines on Data Protection Impact Assessments and determining whether processing is "likely to result in a high risk activity" for the purposes of Regulation 2016/697* <https://ec.europa.eu/newsroom/article29/items/611236>. Similarly, employers can't rely on consent to process employee data and must rely on another legal basis in Art 6 (see *Opinion 2/2017 on data processing at work* <https://ec.europa.eu/newsroom/article29/items/610169/en>

[23] For example, a number of Australian businesses are requiring employees to provide biometric information to manage access to premises or record attendance. These businesses often rely on the employee's consent, which we contend would be vitiated given that the businesses do not provide a suitable alternative. However, these practices are not currently being addressed by any legislation.

[24] Recent examples of where employee personal information was the subject of a data breach include at Rio Tinto and Telstra.

We are concerned that one of the outcomes of the News Media Bargaining Code (NMBC) is that media organisations are increasingly behaving like digital platforms with regard to their data generation and handling practices, in turn having an impact on people's right to privacy. We note that the ACCC's Digital Platform Inquiry recommended *both* the and the NMBC be implemented, such that privacy reform is necessary in order to achieve the aims of the NMBC.

We welcome proposal 9.4 to ensure that media organisations comply with the data security and deletion requirements of APP 11.

Recommendations

10. Abolish the small business exemption, the political party exemption, and the employee records exemptions. Introduce limited exceptions to relevant APPs where necessary.

11. Adopt the proposed updates to the journalism exemption.

Direct right of action and a statutory tort for serious invasions of privacy

We support the development and implementation of both a direct right of action as well as a statutory tort for serious invasions of privacy. Both of these long-standing recommendations would assist with providing additional avenues for redress for individuals upon suffering a privacy-related harm.

We are concerned that the gateway model described in (d), (e), (f) and (g) may be too onerous. Complainants should not be required to make use of the OAIC conciliation process, but it should be an option. Forcing complainants to first go through the OAIC would create a significant and unnecessary burden for that office and risks delay and costs for individuals. In comparable regimes, such as discrimination legislation, the complainant is given a choice and we think a similar approach ought to be taken here.

We are also concerned about the ability of individuals to effectively exercise their rights under these models. It is likely that some of the barriers that individuals will face include: (a) costs associated with litigation; (b) lack of understanding of privacy legislation; (c) already being burdened by having to take steps to protect themselves from harm and not having capacity (resources) to litigate. We would recommend that the government investigate methods that would increase

accessibility, which could include specific recommendations in respect of costs, funding for public education and a requirement to explain avenues for redress in disclosures made by organisations that have interfered with an individual's privacy.

Penalties

We refer to chapter 25, which makes several proposals in respect of civil penalty provisions. We think that these penalties should also be available to individuals who have experienced an interference with their privacy.

Provided that a direct right of action is introduced, we believe it would be appropriate to introduce parallel provisions to those contained in section 546 of the *Fair Work Act*. These provisions allow penalties, in the case of a contravention, to be awarded to a particular person, which is usually the person who has complained of the contravention. A similar provision in the *Privacy Act* could be introduced to allow a civil penalty to be awarded to a person who complains about an interference with his or her privacy.

We make this suggestion because of the significant challenges for victims of data breaches associated with demonstrating harm associated with interferences with privacy. Often the harm associated with interference with privacy is difficult to articulate and hard to attribute to a single act of an organisation. Indeed, for example, a victim of the Optus, Medicare and Latitude data breaches is in a worse position than a person who is affected by only one, and yet it is not clear that a court would consider this. Courts are put in a difficult position to assess harm, and complainants would be required to marshall significant resources to demonstrate a causal relationship with the privacy interference. This risks diminishing the deterrent effect of the reforms to introduce a direct right of action.

We note that section 80U of the *Privacy Act* triggers section 82(6) of the *Regulatory Powers (Standard Provisions) Act 2014*, which requires that courts consider loss and damage suffered because of a contravention when determining the penalty. To avoid the problems arising as outlined above, the legislation could set a minimum amount as a penalty for interferences.

We note that California has a civil penalties provision in their equivalent law which achieves this aim. California's Consumer Privacy Act section 1798.150 provides a right that is substantially similar in effect to the protection offered to APP 11. We note that the relief available is as follows:

> *Consumers may recover injunctive or declaratory relief and damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater.*

A similar provision for individuals who complain of an interference with their privacy would be appropriate and put us on par with comparable jurisdictions.

Recommendations

12. Allow complainants the choice as to whether to file a complaint first with OAIC (before a court action can commence) or directly to a court.
13. Implement both a direct right of action *and* a statutory tort for serious invasion of privacy.
14. Introduce a power to award civil penalties to individuals who have experienced an interference with their privacy as part of a direct right of action.

Rights of the individual

At DRW we support the development of a rights-based approach and the development of a rights culture in Australia. As such, we welcome the expansion of existing and creation of new rights for individuals to be able to exercise control over their personal information.

We do note, however, that proposal 18.9 establishes an exception to these rights and we wish to highlight that care should be taken to ensure that "reasonable steps" cannot be leveraged by organisations to undermine or avoid the requirement to comply with these new rights.

Recommendations

15. Implement the range of new or expanded individual rights, ensuring that organisations cannot avoid meeting the requirements by leveraging or manipulating the meaning of "reasonable steps".

Direct marketing, targeting, and trading of data

First, we wish to note that should the definition of personal information be properly addressed (see pages 5-6), many of the issues we are concerned about raised in chapter 20 of the Report would be addressed or minimised.

Nonetheless, we don't accept that there is a mandate to introduce a regulatory regime for targeted advertising — most people do not want direct marketing, targeted advertising, or data trading. Those that do want to participate in this industry have the option of opting in.

As such, while we welcome proposals 20.2 and 20.3 to allow for people to opt out of their personal information being used for direct marketing or targeted advertising purposes, we do not see this as going far enough. Under these proposals, the burden remains on individuals to opt out of harmful practices, which is unreasonable. Individuals should be required to opt-in before their personal information is used for these purposes.

We are also concerned that the proposals do not challenge the data broker industry in any meaningful sense, but rather enable it.

There are many harms that can occur as a result of targeted advertising, direct marketing and hyper personalisation of content. One area where this is particularly pronounced is in the promotion of harmful or addictive products online. The Foundation for Alcohol Research and Education (FARE) has conducted research on the impacts of digital marketing upon people who are seeking to reduce alcohol, gambling, and unhealthy foods and found that over 80% of participants felt that seeking marketing for these products online made it harder for them to reduce their consumption.[25]

Leaked Meta documents show that Meta gathered psychological insights on almost 2 million children in Australia and New Zealand to sell targeted advertising. This included monitoring children in real-time to identify their current mood, including when they feel 'overwhelmed' and 'anxious', to sell targeted advertising.[26]

We are disturbed by the discussion regarding proposal 20.4 in the Report which notes that:

---

[25] Foundation for Alcohol Research and Education. Experiences with online marketing of alcohol, gambling and unhealthy food: A survey. Canberra: FARE; 2023 Feb. Available from: https://fare.org.au/experiences-with-online-marketing-of-alcohol-gambling-and-unhealthy-food-a-survey/.
[26] Davidson D. Facebook targets 'insecure' young people. The Australian. 2017 May 1. Available from: https://www.theaustralian.com.au/business/media/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6.

> *"requiring consent would not prohibit digital platforms from sharing personal information, but it would ensure that individuals are informed and have agreed to the disclosure of their personal information to a third party"*

And that:

> *"Where consent to trade in personal information was made a condition of accessing goods or services, an APP entity may need to demonstrate that the trading of personal information is reasonably necessary for its functions or activities if an individual objected to their personal information being traded"*

Taken together, it appears that the Report takes no issue with — and does not seek to prohibit or even lessen — the actual practices of data brokers, data intermediaries, or digital platforms which profit from the generation, extraction, commodification and trading of personal information with little to no regard for people's privacy, safety or digital security, nor the ongoing social or political harms caused by such practices.

While transparency is important, simply ensuring that "individuals are informed and have agreed" completely overlooks the immense power imbalance between individuals and data-centric companies such as data brokers and major digital platforms. It means nothing if people have no genuine ability to choose.

What's worse, the implication that consent can be made a condition of accessing goods and services flies in the face of what genuine, valid consent is, further entrenches the imbalance of power between individuals and companies, and contradicts one of the ACCC's key recommendations underpinning the review of the Privacy Act (see page 9 for further discussion regarding consent).

We also echo the concerns of law academic Katherine Kemp with regard to the use of 'dark patterns' in response to proposal 20.3:

> *"Although having the option to opt out of seeing targeted ads gives consumers some limited control, companies still control the "choice architecture" of such settings. They can use their control to make opting out confusing and difficult for users, by forcing them to navigate through multiple pages or websites with obscurely labelled settings."*[27]

We echo the position of CHOICE, which proposes that trade in personal information should be outright prohibited, as the practice carries significant

[27] Katherine Kemp, "Proposed privacy reforms could help Australia play catch-up with ther nations, but they fail to tackle targeted ads," *The Conversation*, February 2023. https://theconversation.com/proposed-privacy-reforms-could-help-australia-play-catch-up-with-other-nations-but-they-fail-to-tackle-targeted-ads-200166

risk of data breachs, exploitative practices and misuse, and deprives individuals of agency and value over their own data.

Recommendations

16. Any direct marketing or targeted advertising should be opt in. Ensure that consent cannot be forced by way of tying it to the provision of goods and services.

17. Amend proposal 20.4 to prohibit the trade in personal information.

Children's privacy

While we generally support the principles contained in the UK Age Appropriate Design Code and do not take issue with the development of a Children's Online Privacy Code in Australia, our concern rests with the possible *implementation* and *compliance* with the requirements that may be contained in such a code.

Specifically, we are concerned that compliance requirements may lead to the development and implementation of widespread age verification processes in order to differentiate between children and adults using online platforms and services.

It is essential that privacy, security and safety for <u>everyone</u>, including children, is not undermined in the process of attempting to increase privacy protections for children.

Digital Rights Watch has previously highlighted many of the privacy and digital security risks and challenges with regard to age verification and age assurance:

- Submission on the draft Online Privacy Bill, which included a requirement for social media companies to verify the age of individuals,[28]
- Submission to the eSafety Commissioner regarding the development of the Restricted Access System Declaration and the roadmap to age verification for online pornography,[29]
- Submission to the Inquiry into Social Media and Online Safety[30]

[28] Digital Rights Watch submission to the Attorney-General's Department on the proposed *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021,* December 2021. https://digitalrightswatch.org.au/wp-content/uploads/2021/12/Submission_-Privacy-Legislation-Amendment-OP-December-2021.pdf

[29] Digital Rights Watch submission to the eSafety Commission on the draft Restricted Access System declaration and roadmap for age verification for online pornography, November 2021. https://digitalrightswatch.org.au/2021/11/25/submission-draft-restricted-access-systems-declaration/

[30] Digital Rights Watch submission to the Select Committee on Social Media and Online Safety on the Inquiry into Social Media and Online Safety, January 2022.

In particular the question of the level of certainty required is important, as reflected in point 4 of proposal 16.5: "whether entities should be required to 'establish age with a level of certainty that is appropriate to the risks' or apply the standards in the Children's Code to all users instead."

Generally speaking, the higher the level of certainty or accuracy of age verification, the more risks it creates with respect to privacy and digital security. For example, many platforms and websites already ask users to provide a date of birth, however this can be readily bypassed with false information, making it less accurate or effective as age verification. Processes for age verification involving the use of official identity documents, cross-referencing with other databases to check age, or facial recognition technology, all require the collection, use or disclosure of additional personal information and in doing so create disproportionate privacy and digital security risks.

As such, while we support, on principle, increased privacy protections for children, we strongly reject any implementation which would create mandatory or widespread age verification practices. Doing so would undermine privacy for everyone in an effort to enhance it for children.

We were pleased to see that the Report acknowledges that in some instances, parental controls can be used to unreasonably limit the autonomy and privacy of children from their parents. We would add that in defining a child as under 18 years of age, subjecting older teenagers to the same controls as those who are much younger is not reasonable. In addition, an astounding amount of stalkerware products and services are marketed as safety products for parents to keep tabs on their children, but are in turn weaponised against other vulnerable individuals or groups. We caution the Attorney-General's Department to take care in balancing these factors when seeking to enhance child safety.

Recommendations

18. Do not require or incentivise the implementation of age verification.

https://digitalrightswatch.org.au/wp-content/uploads/2022/01/Digital-Rights-Watch_Social-Media-and-Online-Safety-Inquiry-2022.pdf

Contact

Samantha Floreani | Program Lead | samantha@digitalrightswatch.org.au