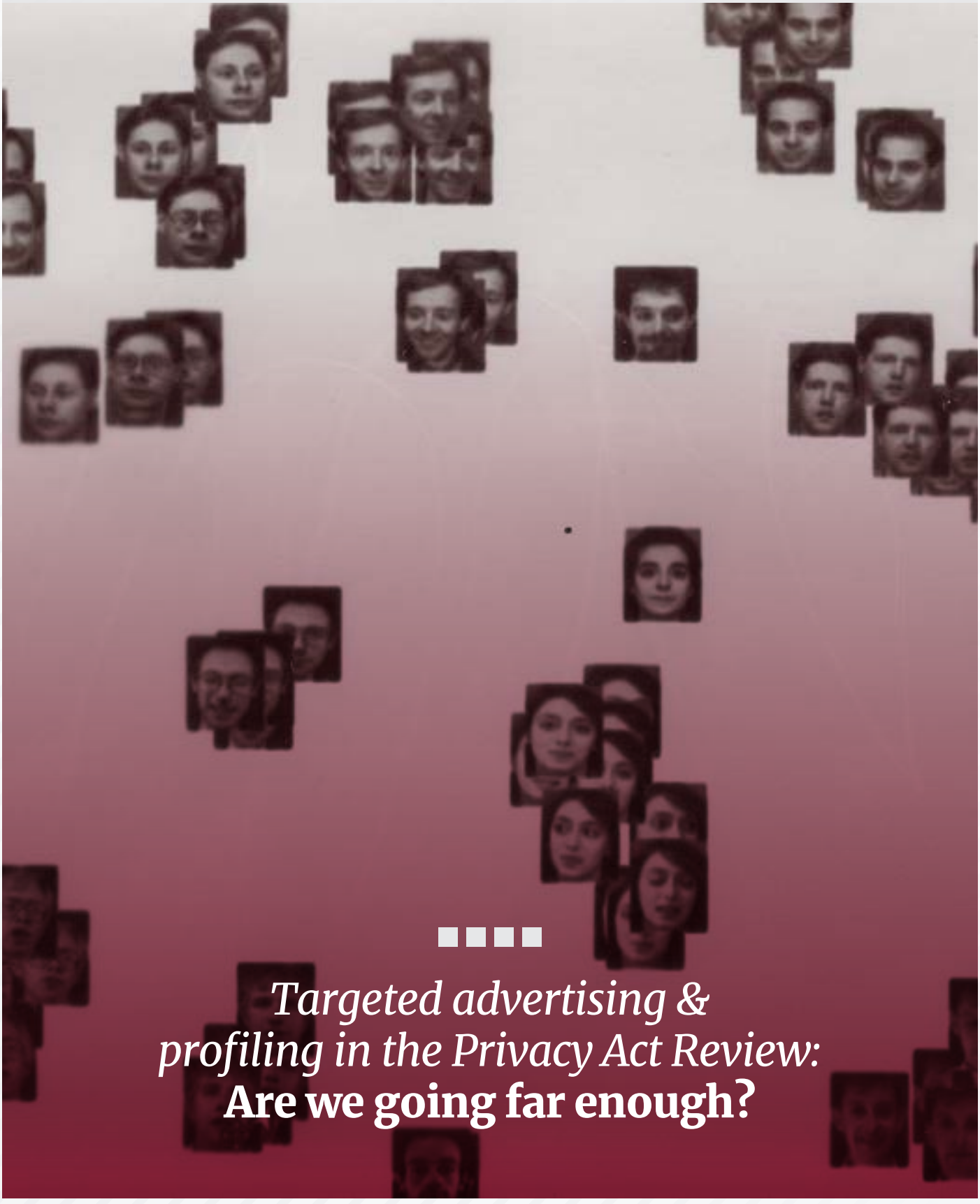
Reset.
AUSTRALIA

Reset.Tech Australia
September 2023 | Policy briefing



Targeted advertising & profiling in the Privacy Act Review: **Are we going far enough?**

Table of Contents

Reset.
AUSTRALIA

Philipp Schmitt & AT&T Laboratories Cambridge / Better Images of AI / Data flock (faces) / CC-BY 4.0

Reset.Tech Australia is an independent, non-partisan policy research lab committed to driving public policy advocacy, research and civic engagement to strengthen our democracy within the context of technology. We are the Australian affiliate of Reset, a global initiative working to counter digital threats to democracy.

Introduction	3
1. Can targeted advertising and profiling coexist with human rights?	5
2. How do we explain the extent of profiling in Australia?	6
3. What do Australians want when it comes to targeted advertising?	7
Discussion	8
Recommendations	13
Acknowledgements	14

Introduction

This policy briefing reflects discussions held in a roundtable of 16 policy experts around privacy, human rights and consumer law on the 4th September 2023. The event was held under Chatham House Rules, and this briefing presents an overview of the discussion. The roundtable was prompted by proposals put forward in the *Privacy Act Review*[1] and the significant pushback from adtech and media against these reforms. Specifically:

The *Privacy Act Review* makes a number of proposals that would curb targeted advertising and its associated profiling.

- Proposal 20.3 provides 'individuals with an unqualified right to opt-out of receiving targeted advertising', and;
- Proposals 20.2 provides individuals 'with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes. Similar to the existing requirements under the Act, entities would still be able to collect personal information for direct marketing without consent, provided it is not sensitive information and the individual has the ability to opt-out'.

These proposals **align with existing requirements in EU regulation and legislation in some US states,** specifically California, Colorado, Texas and Montana, which, combined, cover 20% of the US population.[2]

The **pushback from tech and media has been extensive.** In May 2023, for example, Meta flew the global director of their Privacy Policy team out to lobby against some of the reforms. They claimed the proposals went 'beyond any other any country',[3] and that Meta might need to move 'towards subscription fees'[4] or other 'less desirable choices' if they were adopted. Notably, a subscription model has not been raised as a result of opt-outs provided in Europe, California, Colorado, Texas or Montana.

Against this backdrop, Reset.Tech Australia convened a roundtable to explore the impact of targeted advertising and profiling on Australians from a rights and consumer-based perspective and posed the challenging question: **should we ask for even stronger proposals than the *Privacy Act Review* suggests**?

Three key questions provoked the discussion. These questions, some background polling, and the discussion, are all summarised on the following pages.

---

1. Attorney General's Department 2023 *Privacy Act Review Report* https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

2. In the EU, via the GDPR, where the European Data Protection Board rules that people did not consent to having their data used for targeted advertising when they clicked 'agree' bundled together with the terms of service. This left digital platforms changing the legal basis for processing data for advertising to 'legitimate interests', but this changed legal basis requires giving users choice. See for example, Ryan Browne 2023 'Meta fined over $400 million by top EU regulator for forcing users to accept targeted ads' CNBC https://www.cnbc.com/2023/01/04/meta-fined-more-than-400-million-in-ireland-over-eu-privacy-breaches.html. In the US, California, Colorado, Texas or Montana have all passed laws that require user choice around targeted advertising, via the *California Consumer Privacy Act*, the *Colorado Privacy Act*, the *Texas Data Privacy and Security Act*, and the *Montana Consumer Data Privacy Act.*

3. Sam Buckingham-Jones 2023 Privacy overhaul 'goes beyond any other any country' Australian Financial Review https://www.afr.com/companies/media-and-marketing/privacy-reforms-undermine-businesses-using-instagram-facebook-meta-20230517-p5d92k

4. Paul Karp 2023 'Meta warns Australia's plan to limit targeted ads could push free platforms towards subscription fees' The Guardian https://www.theguardian.com/technology/2023/may/18/meta-warns-australia-platforms-facebook-instagram-harmed-by-limiting-targeted-ads

Public opinion

As background for the roundtable, Reset.Tech commissioned YouGov to poll 1,098 people in July 2023 about targeted advertising, finding that:

1. **There is widespread public support for proposals to provide users with the choice.** 93% agree that people should have the choice to opt-out of targeted advertising.

2. **Australians will take the opportunity to opt-out of targeted advertising.** 82% of Australian adults say they would take the opportunity to opt-out of targeted ads on one or more digital platforms if the choice was available, with only 10% saying they would not.

3. **Australians find targeted ads intrusive, not helpful.** Adtech companies often describe targeted advertising as helpful to consumers. However, only 20% of people find targeted advertising very or somewhat helpful, while 73% find it very or somewhat intrusive.

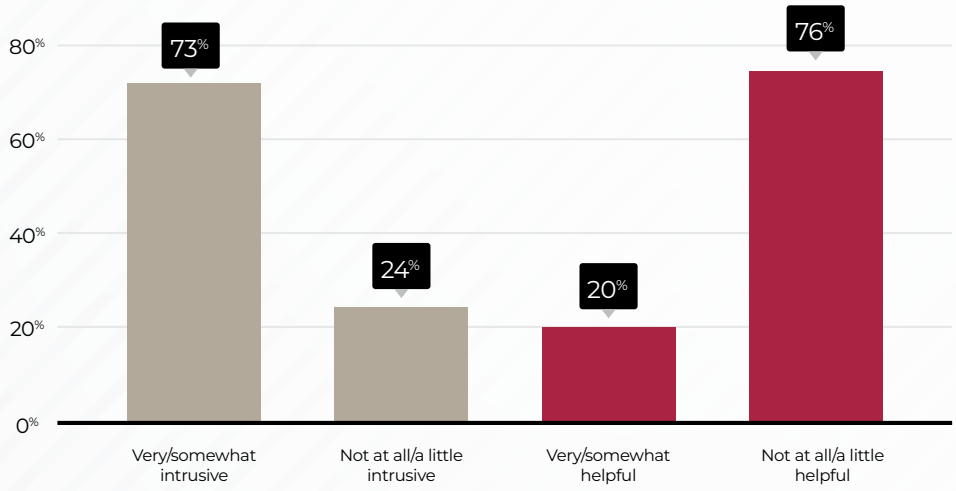


Figure 1: Responses to the questions 'Do you find targeted ads intrusive' and 'Do you find targeted ads helpful' plotted side by side. 'Don't know' is not graphed. (n=1,098)

4. **People identify a wide range of concerns around targeted advertising.** These include:
   - **Consumer privacy concerns:**
     - 90% would prefer less information was collected about them online for advertising.
     - 87% would prefer platforms stop targeting ads based on sensitive personal information such as their political views, sexuality, or health.
     - 84% would prefer platforms stop targeting ads based on online browsing history.
   - **Pervasiveness:** 73% said they often receive targeted ads for things they find themselves 'just thinking about'.
   - **Irrelevance:** Only 27% said that they read or watch the ads served to them by targeted advertising, which suggests they are of little relevance or interest to consumers.
   - **Adversely affects brand loyalty:** Only 23% of respondents said they like brands more when they are targeted and routinely receive ads from brands.

1. Can targeted advertising and profiling coexist with human rights?

The last decade has witnessed a shift from traditional advertising to personalised advertising, with profound impact. Personalised advertising works by using millions of data points on each and every one of us to create real-time profiles of our personalities, preferences and emotional vulnerabilities, which are then used to tailor advertising. This is quite different from traditional, contextual advertising.

Advertising, profiling and targeting involve personal data; therefore, personal data protection and privacy are key considerations. These are not just important as standalone rights but also operate as gateways to other rights. These include the right to freedom of thought and opinion, both of which are threatened by unregulated targeted advertising.

Since being established in the *Universal Declaration of Human Rights*, very little work has been done on freedom of thought or opinion. This lack of attention may be partly because, for a long time, it was widely believed that freedom of thought and opinion could not be easily affected by people, businesses or the government. The dawn of online profiling highlights the untruth of that: whether or not it works, the idea is that our thoughts can be observed, tracked and used to change the way we think and behave. Current regulatory frameworks are not fit for purpose, and there is cause for concern regarding freedom of thought and opinion.

Freedom of thought is one of the very few absolute rights in international human rights law. Violations can never be justified. However, the adtech system collects data about individuals on a massive scale specifically in an attempt to violate these rights.

Targeted advertising often becomes manipulation.[5] By its very nature, like all advertising, it is designed to persuade. But there is often a blurring of the line between persuasion and manipulation. The way targeted advertising is deployed, i.e. through finding our weaknesses and vulnerabilities by using extensive data sets, is often designed to bypass our conscious faculties. In this way, it becomes manipulation, which is evident when we see adtech and data brokers pushing information about vulnerabilities to marketers on everything from children's interest in extreme weight loss[6] to people's heavy gambling habits.[7] We have the right to not be penalised for our thoughts, but the adtech system does exactly this.

There can be severe consequences when we allow actors to manipulate populations and individuals. The example of Cambridge Analytica showed us that manipulation can be politicised and violate rights.[8] This can also drive an ecosystem of misinformation and disinformation, with profiling and targeting serving up increasingly extreme and polarising views. Likewise, Myanmar highlighted how dangerous this can be.[9]

---

5. Literature differentiates manipulation from persuasion when it subverts decision-making processes. (See for example Daniel Susser, Beate Roessler Helen Nissenbaum 2019 'Online Manipulation: Hidden Influences in a Digital World' Georgetown Law Technology Review 1 et al https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3306006). This literature would suggest that target advertising can amount to manipulation, especially when targeted at vulnerable groups whose decision-making processes are already impaired.

6. Reset.Tech 2023 Profiling children for advertising https://au.reset.tech/news/profiling-children-for-advertising-facebooks-monetisation-of-young-peoples-personal-data/

7. Ariel Bogle 2023 'Heavy TAB gamblers' among groups targeted by online advertising database The Guardian https://www.theguardian.com/australia-news/2023/aug/15/tab-gamblers-betting-australia-targeted-microsoft-xandr-advertising-database

8. See for example Emma Briant 2020 *Cambridge Analytica Interactive Map* https://www.propagandamachine.tech/ca-map

9. Melanie O'Brien & Julia Powles 2022 'Facebook's meta complicity in the Rohingya genocide' ABC https://www.abc.net.au/religion/facebook-complicity-in-the-rohingya-genocide/13737882

2. How do we explain the extent of profiling in Australia?

Australians are monitored en masse by a complex data industry, which exists largely to service ads. There are the giants, like Google and Facebook, operating in Australia's distributed data industry, but there are also many smaller companies, including publishers, advertisers and data brokers (intermediaries). Active data brokers in Australia range from large companies like Roy Morgan and Experian to smaller companies like Lifesight and AlikeAudiences, which sell particularly sensitive information such as geofenced location data.

The Xandr file, a data set made public for a short while in 2021 by Microsoft, lists some of the more than 650,000 characteristics that people can be targeted with. To be precise, it lists the 'audience segments' that data brokers hold, where segments are characteristics (like low income, heavy gamblers, etc.), and these are tied to digital identifiers data brokers use to identify individuals. Digital identifiers, such as smartphone device numbers, cookie IDs, and browser IDs, are always tied to an individual person, and often this data follows people across the digital world.

This data is often sensitive and powerfully comprehensive. Characteristics documented include age; gender; occupation; rent; loans; purchases; preferences; commutes; lifestyles; geofenced characteristics, like those who have entered an Oporto or a Woolworths; and purchasing characteristics such as through loyalty programmes, etc. All of this excessive data harvesting contributes to expanding data flows.

Mobile apps can expose exact movements to data brokers, which can then resell the movements to third parties. Data on people (including teenagers) visiting mosques, schools and hospitals is collected and sold. Little is known about these data flows.

Advertisers pay for the ability to exploit the data, funding an uncontrolled surveillance machine wherein data brokers can resell data to anyone, from the government to criminals. This creates the uncontrolled data flows that characterise the current data ecosystem.

Moreover, much of the data is flawed. Flawed data is likely to generate inaccurate predictions about people, which can limit or affect their choices. Nearly everything we do affects what products are displayed to us online and what prices we receive.

In the end, all of this data attaches a particular attribute to a particular identifier, and thus to a particular person. Linked data sets therefore pose unique privacy risks due to their comprehensive and extensive nature.

---

10. Yadullah Abidi 2023 ' Over 650,000 audience segments' found on Microsoft's ad platform Xandr' Candid https://candid.technology/microsoft-xandr-650000-audience-segments/'

3. What do Australians want when it comes to targeted advertising?

There is a mismatch between what businesses tell us Australians want for targeted advertising and what Australians actually want. Businesses are using our data in more ways than ever before. Prices and options offered to consumers today are all features of targeted advertising. But do Australians really care?

Recent research from the Consumer Policy Research Centre (CPRC)[11] found Australians are not comfortable with practises happening right now:

- **74% are not comfortable with companies sharing or selling personal information with other companies.**
- **79% agree that a company should not sell people's data under any circumstances.**
- **64% find it unfair that companies require us to supply more personal information than is necessary to deliver a product or service, and;**
- **90% expect businesses to protect people's information from being used in ways that leave them worse off.**

Australians are generally not okay with the status quo. They have a high level of discomfort with online monitoring in general, and once it flips into targeted advertising, that discomfort compounds. Even Australians who are comfortable with some form of online monitoring and targeting are generally looking for better protections.

A range of interventions are possible, including:

- **Stricter laws** against unfair business practices in order to protect consumers from data extraction and digital misuse. A long-anticipated consultation about this was recently released,[12] which suggests potential movement.
- **Modernised privacy laws.** The *Privacy Act Review* may enhance privacy protections, which could help reduce the worst excesses of targeting advertising and stem the uncontrolled data flows that emerge around this.
- **More resources for enforcement.** Even strong laws are insufficient if they are not properly enforced. Regulators need to have the power and resources to act on complaints and to start investigations into problematic data practices out of their own volition.
- **Better redress.** There is a need to create clear and easier pathways for individuals to access remedies when digital harm occurs.

---

11. CPRC 2023 Not a Fair Trade https://cprc.org.au/not-a-fair-trade/

12. Treasury 2023 Unfair trading practices - Consultation Regulation Impact Statement https://treasury.gov.au/consultation/c2023-430458

Discussion

Need for improvements to current proposals in the Privacy Act Review

- **There is a need for protections that are not only much stronger than we currently have but also stronger than the proposals in the *Privacy Act Review* report.**

Opt-ins over opt-outs

- The *Privacy Act Review* report puts forward stronger protections for particular groups and an opt-out right. But ultimately, an opt-out right still rests on a consent model where the onus is on the user to take steps to protect their privacy.[13] There is, however, increasing recognition that the consent model is flawed. Consumers are often not sufficiently well-informed to make meaningful choices, or they believe that their choice is not relevant. Newer consumer protection models seek to shift onto data processors the burden of demonstrating the legality and justifications for processing. We start to see that other options are needed.
- With regard to targeted advertising, an opt-in model would be preferable to an opt-out model. People tend to be passive in online decision-making, so an opt-out is not going to afford enough people the protections they require. While in general there has been much talk about 'consent fatigue' used to justify opting people in, there has been little talk about 'objection fatigue', or the effort it takes to exercise your right to opt-out.
- There are potential issues with opt-out mechanisms as well, as we have seen play out in Europe with Meta.[14] If Australia introduces an opt-out model, uptake will depend on how this is operationalised and how the choices are presented. While polling suggests that most people do not like targeted advertising, it will be important to make opt-outs easy to understand and exercise and to frame them in ways that make the choice explicit.
- Polling also suggests that Australian consumers prefer opt-in provisions to opt-out provisions. The onus should not be on consumers to go through and opt-out every single time, and it is debatable whether this onerous obligation constitutes real consent. Given that targeted advertising has significant effects on people's rights, the choice to receive it needs to be an active one.

---

13. See for example Reset.Tech 2023 The Capacity of the Consent Model https://au.reset.tech/news/capacity-of-the-consent-model-online/

14. NYOB 2023 No b*llshit opt-out https://noyb.eu/en/no-bullsht-opt-out-free-noyb-tool-quick-and-broad-facebook-objections

Systemic protections

- A duty of care model can be built into data practices, as can fiduciary models.[15] There are precedents for this, including in the EU's *Digital Services Act* and India's *Digital Personal Data Protection Bill*. These models of policy tangibly shift the onus away from consumers and towards businesses taking responsibility for the implementation of how they are using data.
- Duty of care models can also align different 'policy silos', including online safety policy[16] and consumer protection models. There is also emerging precedent here, such as the UK's *Online Safety Bill*.
- It might also be useful to compare contemporary forms of targeted advertising, which are extremely invasive, to subliminal advertising. This comparison raises two considerations:
    1. Given the risk subliminal advertising poses in its intent to influence people's decisions in ways they are not aware of, it has been banned in the EU and is widely recognised as unacceptable. Intent matters; banning targeted advertising is an option that has been advocated for at the European level,[17] and might warrant discussion in the Australian context.
    2. This EU-wide ban on subliminal advertising applies regardless of whether or not it actually works. The intent alone to manipulate is an attempt to violate rights. There is a precautionary element to this that may be useful in 'future-proofing' regulations. If a technology intends to violate freedom of thought or opinion, it is not necessarily prudent to wait for the harm to happen before regulation steps in. We need to govern for what is coming down the pipeline, not just for what is currently effective.

---

15. See CPRC 2023 In whose interest? Why businesses need to keep consumers safe and treat their data with care https://cprc.org.au/in-whose-interest/

16. See for example Will Perrin & Lorna Woods 2019 Online harm reduction – a statutory duty of care and regulator https://d1ssu070pg2v9i.cloudfront.net/pex/pex_carnegie2021/2019/04/06084627/Online-harm-reduction-a-statutory-duty-of-care-and-regulator.pdf

17. See for example Emma Briant 2022 Challenging Targeted Advertising: Highlights from my European Parliament Visit https://www.patreon.com/posts/75260892?utm_campaign=postshare_creator

Failures of the consent model

- There needs to be a concerted policy movement away from consent as the dominant justification for Australian data processing. One contributor to the roundtable noted that industry and investors are still actively incentivising the development of new uncontrolled data flows under the guise that user consent is enough. For policy to redress this, the model needs to be actively changed. The proposals for a 'fair and reasonable' requirement presented in the *Privacy Act Review* may help, but these would need to be rigorously enforced.
- Current models for collecting consent are so flawed that they point to a real issue with compliance with existing law.[18] Consent is often click-wrapped into 90,000-word privacy policies that are not fit for purpose.
- Consumer education and awareness approaches are equally problematic; consumers should not have to take proactive measures, such as 'educating themselves' and 'selecting the right settings' in order to have their privacy respected. Consumers should have confidence that their data is not being used in ways that harm them without needing to take active measures.
- Privacy is often collective (as the discussion below highlights). Consent models are individual and fail to address the harm that processing one person's data could cause to others. For example, processing biometric data, or 'group data' can lead to collective harm justified on individual notions of consent.

Need for adequate enforcement

- Australia has long had an issue with the slow and inadequate enforcement of privacy rights. While the powers of the Australian Information Commissioner have recently been expanded, there is a need to ensure that enforcement issues do not render meaningless any improvements in policy.
- For example, the existing Australian Privacy Principles already include a general rule that renders data collection from third parties – rather than the individual themselves –unlawful.[19] This is not applied in the context of brokering and targeting advertising. This issue has been raised with regulators over the years with no response.
- This matches a general pattern observed; for example, consumer groups are often advised against raising complaints with the regulator because investigations are slow and enforcement actions are so limited.
- A more robust approach to enforcing privacy regulation is necessary to bring it in line with the enforcement of other Australian consumer statutes, which may require a cultural shift.
- There is an issue around the lack of resourcing for privacy regulators, and any improvements in policy and additional powers need to be resourced.
- The issue is not uniquely Australian. From a policy perspective, the EU's *General Data Protection Regulation* (GDPR) is probably the best instrument when it comes to tackling targeted advertising, but its enforcement is also patchy. Where enforcement is lacking, policy is unlikely to be effective.
- In terms of regulators who are adopting a more robust approach, the US' Federal Trade Commission (FTC) is taking meaningful action to strengthen enforcement, and the European Commission (EC) appears to be stepping into the space of digital regulation where data protection commissions across Europe have been failing. There are examples that Australia could draw from.

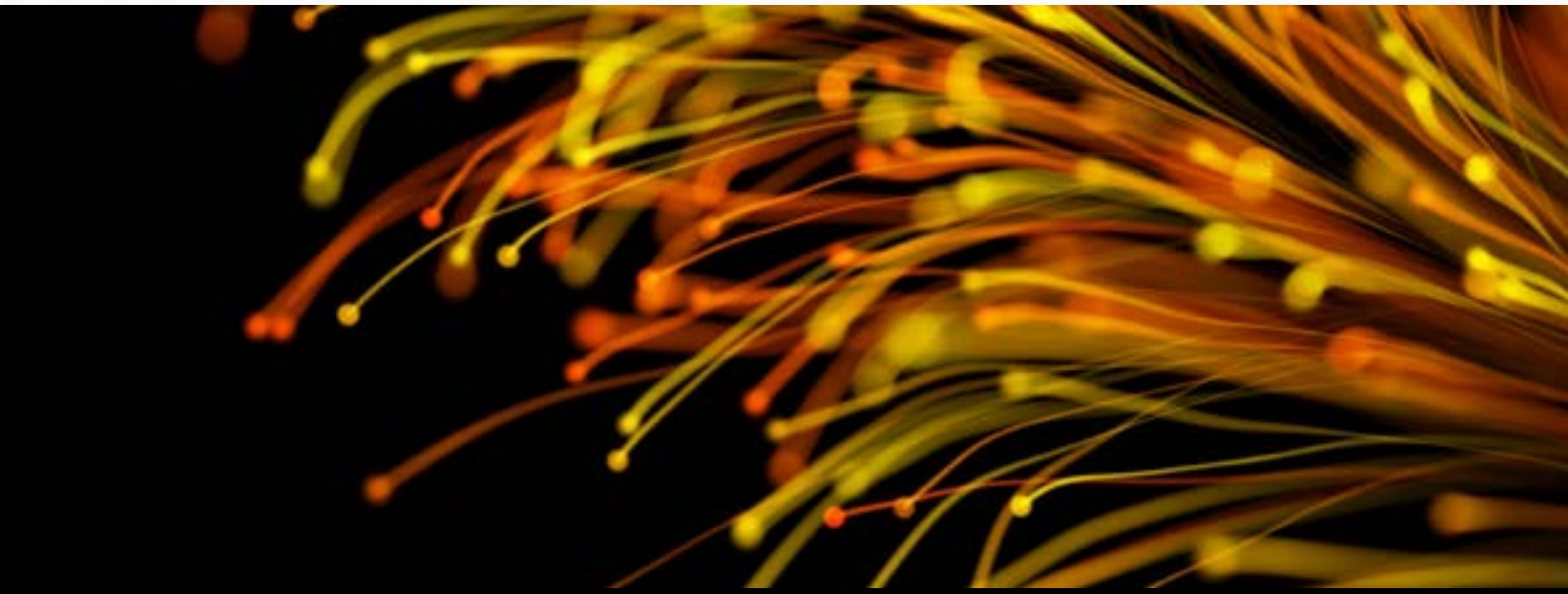
---

18. See for example Reset.Tech 2022 Did we really consent to this? https://au.reset.tech/news/did-we-really-consent-to-this-terms-and-conditions-young-people-s-data/

19. See for example Katharine Kemp 2022 Why we need to enforce existing laws against 'data enrichment' Choice https://www.choice.com.au/consumers-and-data/protecting-your-data/data-laws-and-regulation/articles/why-we-need-to-enforce-laws-against-data-enrichment

Need for proposals to address alternate models of contextual advertising

- Privacy reforms should address not only targeted advertising but also emerging forms of contextual advertising. These can be data-heavy, apply advanced analytics and, without regulation, have the capacity to be invasive.
- It was the dominant mode of digital advertising around 2014, when Facebook launched Lookalike audiences and Google released a similar product. These models shifted away from 'specifying targets' or 'matching consumers' using data from data brokers to probabilistically build audiences based on their associations with each other. This used a range of personal data beyond the specific categories identified. These models raised new issues:
    1. Current models of consent are inadequate for this type of advanced analytic contextual advertising because an individual's data is used not only to analyse and create insights about them but also others (e.g. lookalike data, FLoC etc.). How does our individual approach to consent apply when someone's data will be used to train a model that harms others? Salomé Viljoen (2020) argues that the individual approach to consent misses the relational aspect of how data production is used in today's digital economy, i.e. to put people into population-based relations with each other. Part of what makes an individual's data valuable is what it says about other people. This relational aspect of data production and the harms that come with it call for a move away from individual data subject rights to more collective and democratic forms of data governance. Privacy is an individual as well as a collective good.
    2. Sensitive data and potentially protected characteristics can be difficult to 'protect' under advanced analytic contextual advertising. Even where categories such as ethnicity, political persuasion, sexuality etc. are directly removed, there is the problem of proxies. Probabilistic models do not deal with an explicit category but rather patterns and probabilities, so even if you rule out a protected category, there are more than enough proxies available to recreate it.
- Concerns about contextual advertising are being framed under the guise of 'brand safety', rather than for the purposes of consumer protection. This raises two considerations:
    1. Consumer protection is important but may become overshadowed.
    2. There are potentially shared interests between advertisers wanting brand safety and advocates wanting consumer protection. Both want more fine-grained oversight and control over how contextual advertising works.
- The implications of data-driven contextual advertising require further consideration.



Rights-based approaches

- Freedom of thought offers potential, untested litigation opportunities. The issue was raised in a Spanish constitutional law case involving profiling by political parties. Ultimately, the practice was ruled unconstitutional on the basis of privacy, so the issue of freedom of opinion and thought was not considered in detail.[20] However, there may be potential to develop thinking around this.
- Freedom of assembly and association is also worth considering, especially in the context of policy threats to encryption and shared association.

Broader need for transparency and observability

- There is a real lack of transparency and observability around how personal data is used to drive targeting and profiling. This makes understanding and documenting the harms more difficult and makes regulations harder to enforce.
  - 'Transparency' makes content visible, but 'observability' creates the institutional and technical conditions to allow understanding of how these models work and what their effects are. Accountability requires more than transparency; it requires observability.[21]
  - The dominant approach to transparency in Australia is delivered in the form of ad libraries and annual global transparency reports. However, these do not create the conditions for observability or allow researchers or regulators to see how their models target people at an individual level or an Australian level.

20. See Susie Alegre 2021 Inside Your Head: Defending Freedom of Thought https://digitalfreedomfund.org/author/susie-alegre/

21. See Bernhard Rieder & Jeanette Hofmann 2020 'Towards platform observability' Internet policy review, 9(4), 1-28 DOI: 10.14763/2020.4.1535

Recommendations

The following recommendations have been developed based on the discussion at the roundtable:

- Proposal 20.3 of the *Privacy Act Review*[22] currently suggests that individuals should be provided 'with an unqualified right to opt-out of receiving targeted advertising'. This should be revised to require an explicit opt-in in order to be targeted with advertising.
- A broader duty of care model should be considered for the *Privacy Act* in the upcoming review of the *Online Safety Act*.
- Proposals 12.1 and 12.2 of the *Privacy Act Review* recommend implementing a fair and reasonable test to ensure that data processing is within the bounds of the *Privacy Act*. It needs to be made explicitly clear, either in the Act or through subsequent guidance, that consent does not override the need for fairness and reasonableness.
- Funding for regulators, including the Office of the Australian Information Commissioner, needs to be commensurate with any new powers or expectations under the Act. There should be an expectation that regulators proactively use their investigative powers and respond to complaints in a timely manner.
- Any reforms to the *Privacy Act* need to adequately address potential privacy incursions from advanced analytic contextual advertising. This could be made explicitly clear, either in the Act or through subsequent guidance.
- Reforms to the *Privacy Act* and potentially the *Combatting Misinformation and Disinformation Bill* should consider provisions for researcher access and other heightened measures to create observability.
- Strategic litigation needs to be considered around the rights-based violations emerging from the targeted advertising model, using international human rights law.

---

22. Attorney General's Department 2023 *Privacy Act Review Report* https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

Acknowledgements

This briefing paper reflects the expertise of those who contributed to the roundtable. Attendance does not necessarily mean endorsement. This includes:

- **Susie Alegre, Doughty Street Chambers and author of Freedom to Think**
- **Aruna Anderson, Reset.Tech Australia**
- **Assoc Prof Nicholas Carah, Director of Digital Cultures & Societies, University of Queensland**
- **Wolfie Christl, Cracked Labs**
- **Alice Dawkins, Reset.Tech Australia**
- **Dr Rys Farthing, Reset.Tech Australia**
- **Chandni Gupta, Consumer Protection Research Centre**
- **Assoc Prof Katharine Kemp, Faculty of Law & Justice, UNSW**
- **Dr Kate Mannell, Deakin University**
- **Assoc Prof Ramon Lobato, RMIT University**
- **A. Swetha Meenal, Privacy Lawyer & Founder, Dark Patterns Lab**
- **Matt Ngyuen, Reset.Tech Australia**
- **Assoc Prof Julia Powles, UWA Tech & Policy Lab, UWA Law School**
- **Assoc Prof Normann Witzleb, The Chinese University of Hong Kong and Monash University**
- **Assoc Prof Emma Briant, Monash University**

All errors and omissions rest with Reset.Tech Australia.

Reset.
AUSTRALIA

hello@au.reset.tech