

Submission on the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021

December 2021



About FARE

The Foundation for Alcohol Research and Education (FARE) is the leading not-for-profit organisation working towards an Australia free from alcohol harms.

We approach this through developing evidence-informed policy, enabling people-powered advocacy and delivering health promotion programs.

Working with local communities, values-aligned organisations, health professionals and researchers across the country, we strive to improve the health and wellbeing of everyone in Australia.

To learn more about us and our work visit www.fare.org.au.

You can get in touch via email at info@fare.org.au

FARE is a registered charity, and every dollar you give helps fund projects keeping our communities healthy and safe. You can make a tax-deductible donation at: www.fare.org.au/donate.

Contents

| | |
|---|----|
| About FARE | 2 |
| Contents | 3 |
| Summary of recommendations to the consultation | 4 |
| Restricting data processing for commercial marketing..... | 5 |
| Requirements addressing children and ‘vulnerable groups’ | 6 |
| Enhancing transparency in data processing activities..... | 7 |
| Preventing conflict of interest in developing the OP Code | 8 |
| Ensuring effective enforcement of privacy regulation | 9 |
| References | 10 |

Introduction

Everyone should be able to enjoy the benefits of using digital technologies to work, learn and play. This can happen when we have safe digital environments that enable people's health and wellbeing. However, online platforms have designed digital systems that can create harm.

Every day, millions of people across Australia, including children who are spending an average of over 14 hours online each week¹, are exposed to relentless advertising which targets their specific vulnerabilities, emotions and attributes. This is especially harmful when the products being pushed are harmful and addictive - such as alcohol, tobacco (including e-cigarettes and vapes), gambling and unhealthy food products.

Complex privacy policies and disingenuous 'consent' mechanisms enable online platforms to continue to extensively profile and track people, developing intimate insights into their lives, to increase profit from digital advertising. This commercial cyberstalking enables advertisers to learn people's individual susceptibilities and vulnerabilities to target them with advertising that is most likely to influence their behaviour.

These insights are used by companies selling addictive and harmful products such as alcohol, gambling, tobacco and highly processed foods to aggressively market their products.²⁻⁴ This means that intimate information, such as indicators of individuals experiencing addiction or other related mental health challenges, are being used to disproportionately target marketing to people who are most at risk of harm from these products.

Alcoholic products cause significant harm to Australians. Alcohol use is causally linked to over 200 disease and injury conditions⁵ and nearly 6,000 lives are lost and more than 144,000 people hospitalised from use of alcoholic products each year.⁶ In 2018, alcohol use contributed to 4.5% of the total burden of disease in Australia.⁷ Alcohol is an addictive substance. In 2019, the National Drug Strategy Household Survey found that 10% of people in Australia who had an alcoholic drink in the previous 12 months were likely to meet the criteria for alcohol dependence when assessed by the Alcohol, Smoking and Substance Involvement Screening Test (ASSIST-Lite).⁸

In 2019 the heaviest drinking 5% of the Australian population accounted for 36.1% of all the alcohol consumed (drinking almost eight standard drinks per day) and the heaviest drinking 10% of the Australian population accounted for 54.1% of all alcohol consumed (drinking almost four standard drinks per day).⁹ By design, platforms and companies target advertising to people who purchase or indicate interest in products the most.^{3,10,11} For example, if people are using alcohol products in large quantities, alcohol companies target more marketing material to these people,¹² encouraging them to continue a high level of alcohol use. With harmful and addictive products, this means that this this form of targeting has the potential to cause the most harm.

A privacy-by-design approach is needed. Being commercially cyberstalked should not be the default requirement for using online services. People's wellbeing must be prioritised over commercial profits from unfair and harmful data processing and digital marketing practices.

With digital connection more important in our everyday lives than ever, a regulatory system that ensures a safe and healthy online environment for everyone is essential.

Summary of recommendations to the consultation

We welcome the opportunity to provide a submission on the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (the OP Bill). We support that the OP Bill seeks to cover harmful

data processing practices by online platforms, and that the scope of the OP Bill extends beyond social media platforms to include data brokerage services and large online platforms and enables flexibility to widen this scope if required.

However, the OP Bill is limited in its overall scope. Major privacy reforms are needed to address the harmful data processing practices by online platforms. We recommend that the Government prioritise the Privacy Act review, which will provide an environment that better protects people's privacy, and health and wellbeing, in which the OP Code can then operate. Aligning with this view, we note that some of our recommendations to this consultation speak to broader topics currently being assessed through the review of the Privacy Act. In that context, this submission foreshadows some of the recommendations we will make to the review of the Privacy Act consultation.

To this end, we make the following recommendations for the Online Privacy Bill:

1. Prohibit the collection, use and disclosure of personal information for commercial marketing purposes unless a person has provided active, informed, freely given and non-incentivised opt-in consent.
2. Prohibit the profiling and targeting of children for commercial purposes, and data processing activities by, or for, companies selling or marketing addictive or harmful products.
3. Expand the sections that the Online Privacy Code must address under Australian Privacy Principle 1 on open and transparent management of personal information, including through requiring transparency in models used for digital marketing.
4. Require the Information Commissioner to develop the Online Privacy Code.
5. Resource the Office of the Australian Information Commissioner to conduct regular surveillance and enforcement activities.

We further elaborate on these recommendations in the sections below.

Restricting data processing for commercial marketing

Recommendation: Prohibit the collection, use and disclosure of personal information for commercial marketing purposes unless a person has provided active, informed, freely given and non-incentivised opt-in consent.

Commercial cyberstalking through online platforms – involving the extensive tracking, profiling and targeting of people for commercial marketing purposes – is a major privacy concern, especially when it comes to children and other people who are vulnerable. This concern has been raised in the Privacy Act review discussion paper,¹³ and in the ACCC Digital Platforms Inquiry.¹⁴ However, the current requirements for the OP Code set out in the OP Bill do little to address harmful data-driven marketing practices by online platforms, as is evident by the absence of a requirement to address Australian Privacy Principle (APP) 7, which deals with direct marketing practices. In this regard, the OP Code should require OP organisations to apply APP 7.1, and limit exceptions allowed under other areas of APP 7.

Through extensive data processing, programmatic advertising systems aim to identify people online who are most likely to make a purchase, and to spend higher amounts when doing so.^{3, 10, 11} Companies selling and marketing alcohol pay to access these sophisticated digital systems and tools to aggressively market their products that hurt people's health and wellbeing.² This means that people who already buy and drink alcoholic products in high amounts are the ones that are targeted most aggressively by alcohol companies through their digital marketing practices.¹²

We strongly recommend that the collection, use or disclosure of personal information for commercial marketing purposes is prohibited by OP organisations unless the person has provided active, informed, freely given and non-incentivised opt-in consent.

This approach would require that no personal information is collected, used or disclosed for commercial marketing purposes by default, so that consent is never assumed. This must be facilitated by consent mechanisms that are not designed to nudge or coerce individuals to consent to the processing of their personal information for commercial marketing purposes, for example through bundled consents, 'consent to all' options that incorporate marketing consents, or through requiring consent to process data for marketing purposes to use a service.

Additionally, extra protections should be required so that even where consent has been provided for the collection, use and disclosure of personal information for commercial marketing purposes, OP organisations are required to:

- Ensure that their data processing activities do not pose potential risks of adverse impacts or harm to the person,
- Enable the person to object or withdraw consent at any time and to have information that has been collected for commercial marketing purposes erased,
- Not process sensitive information, such as factors relating to physical or mental health and wellbeing, whether actual, inferred or generated.

Requirements addressing children and 'vulnerable groups'

Recommendation: Prohibit the profiling and targeting of children for commercial purposes, and data processing activities by, or for, companies selling or marketing addictive or harmful products.

The OP Bill Regulation Impact Statement has rightly identified concern that the current harmful data processing practices by online platforms may acutely harm children and people experiencing other vulnerabilities. This is a particularly significant concern when it comes to the marketing of harmful products.

Leaked Facebook documents showed that Facebook gathered psychological insights on almost 2 million children in Australia and New Zealand to sell targeted advertising.¹⁵ This included monitoring children in real time to identify their current mood, including when they feel 'overwhelmed' and 'anxious' to sell targeted advertising.¹⁵ Research has also found Facebook tags children and young people as being interested in harmful products such as alcohol, gambling and junk food,^{16, 17} and approves sponsored content promoting these harmful products to be targeted at children.¹⁷ Further facilitating this harmful marketing to children, Facebook charges approximately \$3 for alcohol advertising to be sent to 1000 Australian children aged 13-17 years old.¹⁷

This results in children being exposed to marketing for harmful products, such as alcoholic products, when they are online.¹⁸ Children's exposure to alcoholic product marketing increases the likelihood that they will start drinking earlier and drink at risky levels.¹⁹ Digital marketing has also been shown to increase positive attitudes and intended and current use of harmful products such as alcohol, tobacco and unhealthy foods.²⁰

The requirements recommended above will help guide online platforms to take more of a privacy-by-design approach, which will provide overarching protections that also act to protect children and other people experiencing vulnerabilities. Additional requirements could also be implemented through the OP Code to

further protect children from particularly harmful practices such as implementing a ‘fair and reasonable’ requirement and prohibiting certain data processing activities.

We support that the OP Code will require services to ensure that data processing of a child’s personal information is ‘fair and reasonable’ in the circumstances (aligning with the recommendation in the Privacy Act review consultation paper), and that the best interests of the child must be a primary consideration when determining ‘fair and reasonable’. The potential risk of adverse impacts or harm (as recommended in the Privacy Act review consultation paper) should also be a primary consideration that is held above other factors when determining ‘fair and reasonable’. Examples of what might constitute ‘fair and reasonable’ circumstances in which a child’s information is processed could include for the purposes of delivering public health social marketing campaigns or personalised educational services.

When considering what is in the best interest of the child, it should be explicit that regardless of consent, the following are not considered to be in the best interest of the child and should be prohibited:

- The profiling or targeting of children for commercial purpose (as per recommendations by the United Nations Committee on the Rights of the Child),²¹ and
- The collection, use or disclosure of children’s personal information by, or for, companies selling or marketing addictive or harmful products, including alcohol, gambling, tobacco (including e-cigarettes/vapes), and unhealthy food.

Any requirement to verify the age of individuals to implement child-specific measures, must be subject to strong privacy controls and be distinct from identity verification. Measures taken to verify age must take a data minimisation approach (i.e., not permit or require OP organisations to collect and triangulate data to determine if an individual is likely a child) and must mitigate any additional privacy risks. To ensure that a privacy preserving system is implemented for age verification, we recommend that the development of an age verification process be led by the Office of the Australian Information Commissioner in consultation with children’s and digital rights stakeholders. It must not be led by industry stakeholders who have commercial conflicts of interest on the matter. Any parental consent verification process should have similar considerations if progressed.

‘Vulnerable groups’

The definition and intent of measures around ‘vulnerable groups’ has not been well defined in the OP Bill and does little to address the overarching issue that, as they are currently designed, online platforms seek to identify and target an individual’s susceptibilities which creates vulnerabilities. Extensive data collection enables online platforms to develop detailed psychometric profiles on people which are combined with detailed accounts of peoples online browsing behaviour.²² These insights are used to tailor marketing activities, including marketing content and messaging, towards specific persuasive susceptibilities of individuals.²² In the case of alcohol marketing, this ability to prey on people’s susceptibilities is particularly harmful as it can disproportionately target vulnerabilities such as dependence. Approaches to address the harms of data processing by online platforms must therefore go beyond simply characterising ‘vulnerable groups’ and address how the system inherently targets and creates vulnerabilities.

Enhancing transparency in data processing activities

Recommendation: Expand the sections that the Online Privacy Code must address under Australian Privacy Principle 1 on open and transparent management of personal information, including through requiring transparency in models used for digital marketing.

Transparency is essential for creating accountability by online platforms about their data processing activities. As it stands, there is little transparency about the breadth and nature of data collection, use and disclosure by online platforms, including when it comes to their marketing models. The drafted OP Bill requires the OP Code to address APP 1.4(c), by requiring OP organisations to have clear and simple explanations about the purposes for which they collect, hold, use and disclose personal information. We recommend that the OP Code should further address APP 1, on open and transparent management of personal information, not solely section 1.4(c).

Particularly, the OP Code should further address requirements for OP organisations to manage personal information in an open and transparent way (APP 1.1) and set out how OP organisations will comply with the APPs (APP 1.2). The OP Code should also require clear and simple explanations by OP organisations addressing:

- The kinds of personal information that the entity collects and holds (APP 1.4(a)),
- How personal information is collected or generated (APP 1.4(b)), and
- How an individual may access and seek correction of this information (APP 1.4(e)).

OP organisations should also be required to be more transparent about their marketing models. While digital marketing continues to become increasingly personalised, targeted and ephemeral (i.e., content that is shared for limited short periods of time and then disappears), driven by extensive data processing activities, there is little requirement for transparency in digital marketing practices through online platforms, meaning the true extent and types of digital marketing practices remains largely under the radar.

Without transparency in their digital marketing models, online platforms are not being held accountable for the harm perpetuated by their digital marketing practices. Therefore, we recommend that OP organisations should be required to provide a clear and simple explanation to users about the use of any automated decision system to make predictions, recommendations or decisions about which, and how, marketing content is sent to individuals.

Preventing conflict of interest in developing the OP Code

Recommendation: Require the Information Commissioner to develop the Online Privacy Code

We oppose the current proposal that the process for developing the OP Code will be based on that for the existing APP Code and Credit Reporting (CR) Code, whereby industry will have the first opportunity to develop the OP Code. Having the OP Code developed by the industry it intends to regulate introduces obvious and insurmountable commercial conflicts of interest when it comes to protecting people's data and privacy. This will undermine the intent of the Code and broader privacy reforms.

Online platforms have demonstrated that without legal and regulatory measures that set standards for protecting people from extensive data processing and related harms, and that ensure transparency and accountability, they will continue to promote harm through their platforms – including by facilitating the targeting by harmful industries of people experiencing vulnerabilities, including children. The vested commercial interests of online platforms conflict with promoting a safe online environment.

This has most recently been made evident by leaked Facebook research and documents that show Facebook is aware of how its platforms harm its users, including children, but refuse to take meaningful actions that

counter this because it conflicts with their core business objectives.^{23, 24} Speaking to these issues, former employee of Facebook, Frances Haugen, has stated:

“The thing I saw at Facebook over and over again, was there were conflicts of interest between what was good for the public and what was good for Facebook. And Facebook, over and over again, chose to optimise for its own interests, like making more money.”²³

It is evident from past and present examples, that measures developed by industry are ineffective at meeting the needs of the public interest ahead of their corporate interests. In July 2021, ahead of the UK’s Age Appropriate Design Code coming into force, Facebook announced that they would “*only allow advertisers to target ads to people under 18 (or older in certain countries) based on their age, gender and location.*”²⁵ Following these claimed changes by Facebook, an investigation by Reset Australia found that Facebook continues to harvest children’s data, such as their browsing histories and other online activities, through their Facebook Pixel.²⁶ The Facebook Pixel provides even more information about individuals than the use of traditional third-party cookie tracking.²⁷ There is no legitimate reason for Facebook to do this, other than to fuel their advertising delivery system. In effect, the measure taken by Facebook does nothing to prevent their AI systems from identifying, selecting and targeting children that are most likely to interact with an advertisement based on information about their daily activities.

We understand that the Privacy Act has required the existing codes under the Act to be developed by the industries that they intended to regulate. However, the current consultation paper in the review of the Privacy Act recommends that the Information Commissioner be given the powers to develop codes under the Act without so that industry is not always provided the first opportunity to develop a code. FARE supports this recommendation of the Privacy Act review consultation paper and recommends that the OP Bill provide the legislative means for the OP Code to be developed by the Information Commissioner.

Ensuring effective enforcement of privacy regulation

Recommendation: Resource the Office of the Australian Information Commissioner to conduct regular surveillance and enforcement activities

Effective enforcement measures that seek to hold companies accountable for their data processing activities are essential to ensuring the meaningful implementation of privacy regulations. We support the measures on the OP Bill that enhance enforcement and penalties for privacy breaches by providing by:

- Providing the Commissioner, the power to investigate potential breaches of the OP Code, either following a complaint or on their own initiative,
- Enhancing enforcement powers of the Information Commissioner, and enabling the Commissioners full range of enforcement powers in the event that an investigation finds a breach of the OP Code, and
- Increased penalties for privacy breaches.

These measures are important, although we note that measures must ensure the onus is not on individuals to identify and report breaches of the OP Code. Rather, regular surveillance and enforcement activities by the Office of the Australian Information Commissioner are essential. This means that the Office of the Australian Information Commissioner must be appropriately resourced. Proper resourcing is critical if the Office of the Australian Information Commissioner is to maintain the heightened level of surveillance and enforcement measures needed to address these complex digital environments.

References

1. The eSafety Commissioner. The digital lives of Aussie teens. 2021.
2. Carah N, Brodmerkel S. Alcohol Marketing in the Era of Digital Media Platforms. *J Stud Alcohol Drugs*. 2021;82(1):18-27.
3. Montgomery K, Chester J, Nixon L, Levy L, Dorfman L. Big Data and the transformation of food and beverage marketing: undermining efforts to reduce obesity? *Critical Public Health*. 2019;29(1):110-7.
4. Torrance J, John B, Greville J, O'Hanrahan M, Davies N, Roderique-Davies G. Emergent gambling advertising; a rapid review of marketing content, delivery and structural features. *BMC Public Health*. 2021;21(1).
5. Rehm J, Gmel GE, Gmel G, Hasan OSM, Imtiaz S, Popova S, Probst C, Roerecke M, Room R, Samokhvalov AV, Shield KD, Shuper PA. The relationship between different dimensions of alcohol use and the burden of disease—an update. *Addiction*. 2017;112(6):968-1001.
6. Lensvelt E, Gilmore W, Liang W, Sherk A, T. C. Estimated alcohol-attributable deaths and hospitalisations in Australia 2004 to 2015. Perth: National Drug Research Institute, Curtin University, 2018.
7. Australian Institute of Health and Welfare. Australian Burden of Disease Study. Impact and causes of illness and death in Australia 2018. Canberra: AIHW, 2021.
8. Australian Institute of Health and Welfare. National Drug Strategy Household Survey 2019. Drug Statistics series no. 32. PHE 270. Canberra: AIHW, 2020.
9. Cook M, Mokica-Perez Y, Callinan S. Distribution of alcohol use in Australia. Bundoora: Centre for Alcohol Policy Research, La Trobe University, unpublished.
10. World Health Organization. Monitoring and restricting digital marketing of unhealthy products to children and adolescents. Moscow: Regional Office for Europe, 2018.
11. Hootsuite. The Facebook pixel: What it is and how to use it 2021 [updated Apr 26; cited 2021 Jun 9]. Available from: <https://blog.hootsuite.com/facebook-pixel/>.
12. House A. Dan Murphy's introduces Netflix approach to marketing. *Drinks Trade*. 2019 Dec 5. Available from: https://www.drinkstrade.com.au/dan-murphys-introduces-netflix-approach-to-marketing?utm_medium=email&utm_campaign=TOP+NEWS%3A+Balter+reveals+plans+to+protect+its+brand+following+CUB+sale&utm_content=https%3A%2F%2F
13. Attorney-General's Department. Privacy Act review discussion paper. Australian Government, 2021.
14. Australian Competition and Consumer Commission. Digital platforms inquiry. Final report. Canberra: ACCC, 2019.
15. 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>.
16. Hern A, Ledergaard F. Children 'interested in' gambling and alcohol, according to Facebook. *The Guardian UK*. 2019 Oct 10. Available from:

<https://www.theguardian.com/technology/2019/oct/09/children-interested-in-gambling-and-alcohol-facebook>.

17. Williams D, McIntosh A, Farthing R. Profiling children for advertising: Facebook's monetisation of young people's personal data. Sydney: Reset Australia, 2021.
18. VicHealth. Under the radar: Harmful industries' digital marketing to Australian children. Melbourne: A report prepared by the Victorian Health Promotion Foundation, 2020.
19. Jernigan D, Noel J, Landon J, Thornton N, Lobstein T. Alcohol marketing and youth alcohol consumption: a systematic review of longitudinal studies published since 2008. *Addiction*. 2017;112:7-20.
20. Buchanan L, Kelly B, Yeatman H, Kariippanon K. The Effects of Digital Marketing of Unhealthy Commodities on Young People: A Systematic Review. *Nutrients*. 2018;10(2):148.
21. United Nations Committee on the Rights of the Child. General comment No. 25 (2021) on children's rights in relation to the digital environment. 2021.
22. Winter S, Maslowska E, Vos AL. The effects of trait-based personalization in social media advertising. *Computers in Human Behavior*. 2021;114:106525.
23. Paul K, Milmo D. Facebook putting profit before public good, says whistleblower Frances Haugen. *The Guardian*. 2021 Oct 5. Available from: <https://www.theguardian.com/technology/2021/oct/03/former-facebook-employee-frances-haugen-identifies-herself-as-whistleblower>.
24. Milmo D, Paul K. Facebook disputes its own research showing harmful effects of Instagram on teen's mental health. *The Guardian*. 2021 Sep 30. Available from: <https://www.theguardian.com/technology/2021/sep/29/facebook-hearing-latest-children-impact>.
25. Facebook. Giving young people a safer, more private experience. 2021 Jul 27. Available from: <https://about.instagram.com/blog/announcements/giving-young-people-a-safer-more-private-experience>.
26. Yi-Ching E, Farthing R. How Facebook still targets surveillance ads to teens. Reset Australia, Fairplay and Global Action Plan, 2021.
27. Semerádová T, Weinlich P. Computer Estimation of Customer Similarity With Facebook Lookalikes: Advantages and Disadvantages of Hyper-Targeting. *IEEE Access*. 2019;7:153365-77.



fare
Foundation for Alcohol
Research & Education