Office of the Victorian Information Commissioner

t 1300 006 842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D21/4222

25 February 2021

Digital advertising services inquiry
Australian Competition & Consumer Commission

By email only: AdTechInquiry@accc.gov.au

Dear Digital Advertising Services Inquiry Team,

Submission in response to the Australian Competition and Consumer Commission's digital advertising services inquiry interim report

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to make a submission in response to the Australian Competition and Consumer Commission's digital services inquiry interim report (**report**).

OVIC is the primary regulator for information privacy, information security and freedom of information in Victoria, administering both the *Privacy and Data Protection Act 2014* (**PDP Act**) and the *Freedom of Information Act 1982* (Vic). OVIC also administers the Victorian Protective Data Security Framework (**VPDSF**) and Standards, issued under Part 4 of the PDP Act. The VPDSF sets out the information security standards that apply to the Victorian public sector.

As the Information Commissioner, I have a strong interest in matters that impact on the privacy of individuals, and one of my functions under the PDP Act is to make public statements in relation to such matters. As such, this submission focuses primarily on the proposals in the report that are likely to pose a risk to consumers' privacy.

Targeted advertising

1. Before examining those proposals, it is useful to consider what has caused the imbalance in market power in advertising. As discussed in the report, data is essential to advertising technology (**ad tech**) services and the supply of digital display advertising. Ad tech providers across the ad tech supply chain derive significant value from data. Amongst other uses, data increases the value of ad inventory, it enables advertisers to target advertising to specific consumers or groups of consumers, and it helps ad tech providers measure the effectiveness and performance of ads. OVIC recognises the importance of effective competition in the ad tech sector and acknowledges that the ability to access data not only gives ad tech providers a distinct competitive advantage, but may also create barriers to entry and expansion in the market for other ad tech suppliers.

2. Big platforms have been more successful than traditional media in securing market share because of the data available to them. The success of major data-enabled advertising systems has led to 'micro-targeting,' where advertising spends can be limited to those individuals likely to respond favourably to the advertisement, i.e., being able to show an advertisement to an individual who has previously indicated an interest in certain subjects. While micro-targeting is difficult for traditional media companies, it is trivially easy for new ad tech companies, and it is attractive to advertisers because of its cost effectiveness.

3. The report proposes extending this ability to micro-target to traditional media so as to reduce the competitive edge big ad tech providers currently enjoy. OVIC considers that these proposals would benefit from an exploration of whether micro-targeting is desirable for the community as a whole. Micro-targeting arises from poor privacy practices by major ad tech providers, and the unsupported allegation that consumers want targeted ads.[1] It is only achievable because these ad tech providers are able to skirt privacy legislation by getting consent from consumers for their data, in ways that are ethically problematic and which often rely on consumers consenting to practices with which they are not, in fact, comfortable.

4. Furthermore, there is evidence that providing more data to traditional media companies has the potential to make their systems less effective, not more. Absent certain contextual information belonging to the original platform (which may include date, time, surrounding information, information source, referrer, and other factors), data based solely on user IDs or transaction IDs may have the paradoxical impact of reducing the effectiveness of a targeted advertisement by reducing conversion rates.[2] Thus, while some of the proposals explored in the report may seem attractive, they may create adverse outcomes for advertisers as well as consumers.

5. The ACCC should consider whether effective market competition may be achieved by reducing the power of big ad tech platforms, as opposed to enhancing the power of traditional media by enabling more widespread use of micro-targeting.

Proposal 1 – Measures to improve data portability and data interoperability

6. OVIC agrees that measures to improve data mobility and data interoperability in the market, aimed at reducing data-related barriers to entry, need to be carefully designed. To align with community expectations, data portability measures, involving tools that increase data mobility at the request of the consumer, should provide the consumer with as much control as possible over the sharing and processing of their personal information.[3]

7. As identified in a recent survey on community attitudes to privacy, Australians want more control and choice over the collection and use of their personal information.[4] Importantly, to minimise the risk of data breaches and security incidents, any measures to improve data portability and interoperability should include a clear, legislative, baseline of protections to ensure the safe, responsible and ethical use of data in the ad tech market. OVIC's *Privacy Management Framework*[5] includes examples of baseline privacy protections for the ACCC to consider.

8. With regard to improving data interoperability between ad tech providers, OVIC is concerned that the suggestions to increase ad tech providers' ability to share data are likely to harm consumer privacy. More specifically, OVIC has significant concerns about the proposed Common Transaction ID.

[1] There is research to demonstrate this assertion is false. See, for example, Paul Hitlin and Lee Raine, 'Facebook Algorithms and Personal Data', *Pew Research Center* (online, 16 January 2019) available at: https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/.

[2] Baptiste Kotras, 'Mass personalization: Predictive marketing algorithms and the reshaping of consumer knowledge' (2020) 7(2) *Big Data & Society*, available at: https://journals.sagepub.com/doi/10.1177/2053951720951581.

[3] It should be noted that the ad tech sector, in particular, often relies on "dark patterns" in design to obfuscate the impact of data collection and reduce the ability of consumers to have a meaningful understanding of the purposes and destinations of personal data collected from those consumers. See Harry Brignall, 'Dark Patterns: Deception vs. Honesty in UI Design' (2011) *A List Apart*, available at: https://alistapart.com/article/dark-patterns-deception-vs.-honesty-in-ui-design/.

[4] For further information see the Office of the Australian Information Commissioner's *Australian Community Attitudes to Privacy Survey 2020* available at: https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey/.

[5] Available here: https://ovic.vic.gov.au/privacy/privacy-management-framework/?highlight=privacy%20governance.

Proposal 5 – Implementation of a common transaction ID

9. The report notes that the common transaction ID could help address transparency issues around the pricing of ad tech services by making it easier to track a single transaction across the supply chain.[6] However, given that ad tech providers typically collect large amounts of data about consumers, OVIC is concerned that this proposal would increase the risk of re-identifying a consumer if the common transaction ID is matched with other data held by ad tech providers. De-identified or anonymised data carries the inherent risk of re-identification when matched with other available data.

10. OVIC notes that the privacy and security practices of ad tech providers in the supply chain may vary in sophistication. OVIC suggests that as part of any eventual implementation of the proposed common transaction ID, the ACCC consider imposing a requirement on ad tech providers to demonstrate an ability to comply with overarching privacy obligations as well as any specific privacy provisions, at a minimum. While this would not alleviate OVIC's concerns, it may assist to mitigate some of the privacy risks involved in implementing a common transaction ID.

Proposal 6 – Implementation of a common user ID to allow tracking of attribution activity in a way that protects consumers' privacy

11. The report notes the benefits of the proposed common user ID include increasing the data available to third parties to better track consumers online which would enable advertisers to better assess the performance of their ad campaigns.[7] A common user ID would also improve the ability of ad tech providers to build consumer profiles.

12. Behavioural targeting poses significant risks to consumer privacy and has harmful impacts on society and democracy. For example, if certain advertising or content is only shown to specific groups of people, it can limit meaningful public debate and freedom of thought and expression. In addition, consumer profiling facilitates exclusion and discrimination as it creates an environment where consumers are treated differently based on their profiles.

13. Further, as mentioned in the report, a proposed common user ID may be matched with other information to expose the personal information of users and result in data pooling without an individual's consent.[8] Even if consent was obtained, there are a number of limitations to relying on consent as a means of protecting consumer privacy in a digital environment. For instance, consumers may not read, or engage meaningfully with, the lengthy and often incomprehensible privacy policies and terms of use detailing how their personal information will be collected, used and disclosed. This means that any consent a consumer provides is not likely to meet the requirements for valid consent.[9] Furthermore, consumers may have limited alternatives to accessing a service online so provide consent due to the lack of options.[10]

14. For these reasons, OVIC is of the view that the privacy risks associated with the common user ID are not proportionate to the benefits associated with improving transparency over the performance of ad tech services.

[6] The report, p 183.
[7] Ibid at 185.
[8] Ibid.
[9] The five elements of consent are the individual has capacity to consent, and the consent is voluntary, informed, specific and current.
[10] For detailed discussion on the issues associated with relying on consent, see OVIC's submission in response to the Australian Competition & Consumer Commission's Digital Platforms Inquiry preliminary report available here: https://ovic.vic.gov.au/resource/submission-to-the-australian-competition-consumer-commission-on-the-digital-platforms-inquiry-preliminary-report/.

General comments

15. OVIC notes the discussion in the report on the tension (real or claimed) between consumer privacy, competition and transparency in the ad tech sector.[11] Australian privacy law takes a principles-based approach to regulating information privacy. This is intended to give regulated entities sufficient flexibility to tailor their information handling practices to their specific circumstances while ensuring the protection of individuals' privacy. Rather than being a barrier to sharing information, privacy law promotes sharing in safe, appropriate and proportionate ways. Crucially, building upon privacy principles in the design of any new scheme reduces the risk that any new initiative will breach the social contract governments have with the public. Privacy considerations are therefore a contributor to innovation, not a barrier.

16. Amongst other matters, the ongoing federal review of the *Privacy Act 1988* seeks to make privacy law fit for purpose in the increasingly digital economy and strengthen privacy protections for individuals. OVIC considers that the outcome of this review may impact the proposals in the report, particularly proposals that affect consumer privacy rights.

Thank you for the opportunity to provide comment on the report. My office will watch the progress of this inquiry with interest.

I have no objection to this submission being published by the ACCC without further reference to me. I also propose to publish a copy of this submission on the OVIC website but would be happy to adjust the timing of this to allow the ACCC to collate and publish submission proactively.

If you have any questions about this submission, please do not hesitate to contact me directly or my colleague [redacted], Senior Policy Officer, at [redacted].

Yours sincerely

[redacted]

Sven Bluemmel
Information Commissioner

[11] The report, p 18.