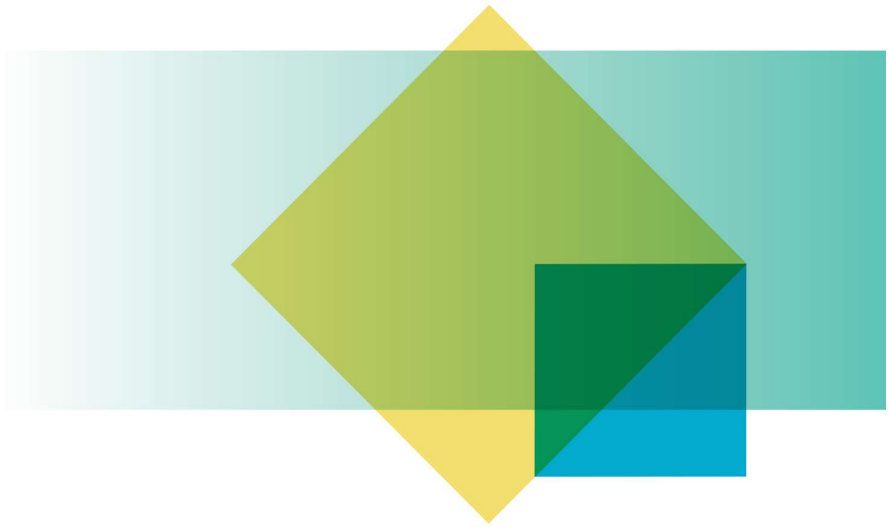
Australian Government

Office of the Australian Information Commissioner

Digital Advertising Services Inquiry – Interim Report

Submission by the Office of the Australian Information Commissioner



Angelene Falk

Australian Information Commissioner and Privacy Commissioner

31 March 2021

OAIC

Contents

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the Australian Competition and Consumer Commission's (ACCC) Digital Advertising Services Inquiry Interim Report (the interim report).

2. The internet has helped to transform the daily lives of Australians, changing the way that individuals interact socially, conduct business and receive services in the 21st century. At the same time, the internet has given rise to new risks, many of which have emerged specifically due to the dramatic increase in the amount of data and personal information collected, used, and shared, both in Australia and globally, to support the internet's targeted advertising-based business model.

3. The interim report recognises the crucial role that data plays in the ad tech system and the important relationship between competition and privacy law in regulating this sector. This echoes the ACCC's Digital Platforms Inquiry final report, which recognised that data-driven markets raise issues at the intersection of privacy, competition and consumer protection considerations.[1]

4. While the operation of Australian privacy law is excluded from the remit of the inquiry, the OAIC notes the significant privacy risks that have emerged as a result of the use of high volumes of data, often involving personal information, by the ad tech industry.[2] These privacy risks have changed significantly in recent years, particularly due to the increasingly complex methods of online targeted marketing involving multiple parties, the increased use of cookies and other online identifiers, and new developments in the way that data is handled which has made it increasingly difficult to draw a bright line between personal and non-personal information.

5. As Government considers reforms to address any competition issues in the ad tech sector, it will be important to consider any implications for the operation of privacy and consumer protection law. In particular, any reforms to competition law should consider the Government's current privacy law reform agenda. This includes the development of a binding online privacy code that will apply to digital platforms and other entities that trade in personal information online, and the review of the Privacy Act, which aims to ensure that Australia's privacy framework empowers consumers, protects their data and best serves the Australian economy.[3]

6. The distinct but complementary roles of competition, consumer and privacy laws also highlight the importance of regulatory co-operation. The OAIC has an effective, collaborative and longstanding working relationship with the ACCC, including through the memorandum of

---

[1] ACCC (Australian Competition and Consumer Commission) (June 2019) *Digital Platforms Inquiry Final Report*, pp 434–435.

This relationship was also recently noted by the European Data Protection Supervisor, who stated that competition, consumer protection and data protection law are inextricably linked policy areas in the context of the online platform economy. For more information, see Wojciech Wiewiorówski (February 2021) *Opinion 2/2021 on the Proposal for a Digital Markets Act [PDF 143KB]*, European Data Protection Supervisor, accessed 1 March 2021, [12]. Also see UK Information Commissioner's Office (2019) *Information Commissioner's Office comments on the Competition and Markets Authority market study interim report into online platforms and digital advertising [PDF 143KB]*, United Kingdom Competition and Markets Authority, accessed 31 March 2021.

[2] For further detail see UK Information Commissioner's Office (2019) *Update Report into adtech and real time bidding* [PDF 779KB], ICO, United Kingdom Government.

[3] AGD (Attorney-General's Department) (October 2020) *Review of the Privacy Act 1988 – Terms of Reference* [online document], AGD, accessed 31 March 2021.

understanding on exchanges of information between these two agencies.[4] The OAIC looks forward to continuing to work with the ACCC on these issues.

7. Given that the operation of privacy law is excluded from the Digital Advertising Services Inquiry, the OAIC's submission is focused on several key proposals in the interim report that are likely to have privacy impacts for consumers.

8. The OAIC notes as a general comment that the right to privacy is not absolute, and in certain circumstances there may be a compelling public interest reason that justifies an impact on privacy in order to achieve other policy objectives. Whether this is appropriate will depend on whether the infringement on privacy rights is reasonable, necessary and proportionate to achieving a legitimate policy aim with a compelling and substantial public interest objective. These considerations will be important in relation to each proposal that has privacy impacts.

9. In assessing whether the privacy impacts of these proposals are reasonable, necessary and proportionate, the ACCC may consider carrying out a privacy impact assessment (PIA).[5] The OAIC has made a specific recommendation to undertake a PIA to assess the privacy impacts of proposals 5 and 6, which the OAIC considers could pose significant privacy risks. PIAs could assist the ACCC to further identify the privacy impacts of their proposals and strategies to mitigate those impacts, building upon the work it has already done in identifying privacy risks in the interim report. The OAIC has several resources on its website that can assist.[6]

10. The OAIC has relevant expertise in assessing privacy risks and developing controls to mitigate privacy risks. The OAIC looks forward to continuing to be consulted in relation to any further development of the proposals discussed in this submission.

Proposal 1 - Measures to improve data portability and interoperability

Data portability

11. Proposal 1 considers creating tools to promote data portability in the ad tech sector, which will 'require firms with a significant data advantage to provide consumers with an easy interface in which to move or share their data from that firm to a third-party at the consumer's request'.[7]

12. The OAIC considers that any data portability scheme should be consumer-led, include appropriate privacy safeguards and be consistent with the Privacy Act and other data portability frameworks, such as the Consumer Data Right (CDR).

---

[4] OAIC (August 2020) *MOU with ACCC — exchange of information* [online document], OAIC website, accessed 18 March 2021.

[5] The OAIC notes that the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Cth) requires Australian Government agencies subject to the Privacy Act 1988 (Privacy Act) to conduct a privacy impact assessment for all 'high privacy risk projects' so this may later be required should the proposals be implemented.

[6] OAIC (May 2020), *Guide to undertaking privacy impact assessments* [online document], OAIC website, accessed 18 March 2021.

[7] ACCC (Australian Competition and Consumer Commission) (February 2021) *Digital Advertising Services Inquiry Interim Report*, p. 80.

A consumer-led approach

13. Data portability is increasingly being implemented in legislative frameworks in Australia and internationally as a mechanism to give consumers greater control over their data.

14. In Australia, the CDR:

- gives consumers a right to data portability in relation to information that has been designated as CDR data
- allows any individual to access information about goods or services in a designated sector that does not relate to an identifiable or reasonably identifiable consumer.

15. An important part of the CDR is that it generally requires consumers to expressly consent to any disclosures, collections and uses of their CDR data.

16. Data portability regimes internationally are similarly consumer-led, with both the European Union's (EU) General Data Protection Regulation (GDPR) and the California Consumer Privacy Act containing a right to data portability at the request of consumers.[8]

17. Accordingly, the OAIC recommends that any data portability right in relation to ad tech should only be with the voluntary, express, informed, specific as to purpose, time limited and easily withdrawn consent of the individual and not exercisable by advertisers or other third parties without this consent.

Privacy Safeguards

18. The interim report acknowledges that data portability raises privacy risks for consumers. Relying on individual requests for a data portability right will require appropriate transparency measures and controls to ensure that individuals can provide valid consent. Strong organisational accountability measures should also be included to reduce the risk of misuse of the personal information, for example, mandating secure transfer methods and other security requirements.

19. The CDR scheme seeks to address privacy risks through obligations around consent, transparency, accreditation and data minimisation. This scheme also expressly prohibits the use or disclosure of CDR data for certain purposes.

20. The OAIC recommends that the ACCC consider the applicability of the privacy-enhancing features of the CDR as a model for developing any new data portability proposals for the ad tech sector.

Interaction with the Privacy Act

21. The OAIC suggests consideration is given to whether any new data portability right could sit appropriately in an existing regime such as the CDR scheme, or whether a new regime should be created. In doing so, it will be important to consider how this right aligns with the purpose of the CDR.

---

[8] Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 ('General Data Protection Regulation'), art 20; *California Consumer Privacy Act of 2018*, 1.81.5 Cal Civ Code § 1798.130 (West 2018).

22. If a separate regime is created, it will be necessary to consider the interaction of the regime with the CDR scheme, the Privacy Act and other global privacy regimes. In doing so it should ensure that the scheme is not unnecessarily duplicative and minimises additional regulatory burden on entities. It will also be important to consider how the regime can be structured to avoid confusion for individuals as to which regime they should use to access their data portability rights.

Data interoperability

23. Proposal 1 also considers measures to increase data interoperability and proposes standardised sharing of non-personal, aggregated or anonymised data in limited circumstances without consent.

24. While enhancing data interoperability may promote competition in the ad tech sector, the interim report acknowledges that this may carry privacy risks. These risks primarily relate to ensuring that this information is appropriately de-identified, and then managing the subsequent risk of re-identification.

25. Information that has undergone an appropriate and robust de-identification process is not personal information and is therefore not subject to the Privacy Act. This requires there to be no reasonable likelihood of re-identification occurring in the context that the data will be made available.

26. Appropriate de-identification may be complex, especially in relation to detailed datasets that may be shared widely and combined with other data sets. In this context, de-identification will generally require more than removing personal identifiers such as names and addresses. Additional techniques and controls are likely to be required to remove, obscure, aggregate, alter and/or protect data in some way so that it is no longer about an identifiable (or reasonably identifiable) individual.

27. This may be particularly challenging in relation to ad tech. As stated in the interim report, bid requests that contain more detailed data will be more attractive. This creates a commercial incentive to continually collect and link information to profiles of individuals, which will likely increase the difficulty in ensuring that this information is able to be appropriately de-identified.

28. Similarly, any sharing of data, even at an aggregated level, increases the risk of re-identification. This is because de-identification is not a fixed or end state. Data may become personal information as the context changes. Managing this risk will require regular re-assessment, particularly if an entity receives additional data, even at an aggregate level, through these data mobility proposals.

29. Accordingly, if the ACCC develops this proposal further, the OAIC recommends that the ACCC have regard to the OAIC's guidance on de-identification as well as the De-Identification Decision-Making Framework, produced jointly by the OAIC and CSIRO-Data61.[9]

30. The requirements around de-identification arise in the Privacy Act Review. The OAIC recently recommended additional protections for de-identified data including:

[9] See OAIC (March 2018) *De-identification and the Privacy Act* [online document], OAIC website, accessed 24 February 2021; CM O'Keefe, S Otorepec, M Elliot, E Mackey, and K O'Hara (2017) *The De-Identification Decision-Making Framework*, OAIC and the CSIRO's Data61.

- Amending Australian Privacy Principle 1 (APP) to insert an express obligation that an APP privacy policy must notify individuals that their information may be anonymised and used for purposes other than those permitted for the initial collection (recommendation 9).
- Extending the obligations of APP 11 to require APP entities to take reasonable steps to protect anonymised information from misuse, interference and loss, and from unauthorised access, modification or disclosure (recommendation 10).
- Introducing a prohibition on APP entities taking steps to re-identify information that was collected by them in an anonymised state, except in order to conduct testing of the effectiveness of security safeguards that have been put in place to protect the information (recommendation 11).
- Extending Part IIIC of the Privacy Act to require notification where:
  - there is unauthorised access to or unauthorised disclosure of anonymised information, or a loss of anonymised information, that an entity holds, in circumstances where there is a risk of re-identification of that information
  - if this information is re-identified, it is likely to result in serious harm to one or more individuals, and
  - the entity has not been able to prevent the likely risk of serious harm with remedial action (recommendation 12).

The OAIC recommends:

- Any data portability right in relation to ad tech should only be with the voluntary, express, informed, specific as to purpose, time limited and easily withdrawn consent of the individual and not exercisable by advertisers or other third parties without this consent.
- The ACCC consider the applicability of the privacy-enhancing features of the CDR as a model for developing any new data portability proposals for the ad tech sector.
- The ACCC consider whether any new data portability right could sit appropriately in an existing regime such as the CDR scheme. In doing so, that it consider how this right aligns with the purpose of the CDR.
- If a new data portability regime is created, the ACCC consider the interaction of the scheme with the CDR scheme and the Privacy Act.
- If the ACCC develops a data interoperability regime, the ACCC have regard to the OAIC's guidance on de-identification as well as the De-Identification Decision-Making Framework, produced jointly by the OAIC and CSIRO-Data61.

Proposal 2 - Data separation mechanisms

31. Proposal 2 considers data separation mechanisms such as data silos, which would prohibit the combining of certain data sets, and purpose limitation requirements, which would prohibit the use of certain data such as health information for ad targeting purposes. The ACCC also proposes additional controls for consumers over how their information is used for an organisation's ad targeting function.

32. The interim report acknowledges that there will be some overlap between this proposal and the Privacy Act to the extent that the relevant data is personal information. That said, while the Privacy Act does create certain requirements and limitations around the use of personal information for direct marketing, it does not contain explicit prohibitions on the combination of data sets or the use of particular types of personal information for direct marketing.

33. It is becoming increasingly clear, however, that some types of information handling practices in the digital age simply do not meet the expectations of the Australian community. For example, the results of the *Australian Community Attitudes to Privacy Survey 2020* showed that 79% of Australians consider an organisation inferring information about them (for example, sexual orientation, mental health, political views) based on what they do online to be misuse.[10]

34. The OAIC's submission to the Privacy Act Review recommended the introduction of full or partial prohibitions on certain information handling practices into the Privacy Act, including:

- profiling, tracking or behavioural monitoring of, or directing targeted advertising at, children
- the collection, use and disclosure of location information about individuals.[11]

35. Similar restrictions have been proposed overseas. In his opinion on the EU Digital Services Act, the European Data Protection Supervisor (EDPS) wrote:

> [T]he EDPS invites the co-legislature to consider further restrictions in relation to (a) the **categories of data that can be processed for targeting purposes** (e.g., limitations regarding the combination of data collected "off platform"); (b) **categories of data or criteria on the basis of which ads may be targeted or served** (e.g., criteria that directly or indirectly correspond with special categories of data or might be used to exploit vulnerabilities); and (c) **the categories of data that may be disclosed** to advertisers or third parties to enable or facilitate targeted advertising.[12]

36. Accordingly, the OAIC supports the ACCC's proposal to restrict or prohibit the combination of data sets or the use of certain information, such as health information, for targeted advertising.

---

[10] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 36.

[11] See OAIC (December 2020) *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, accessed 24 February 2021, pp. 89–92.

[12] Wojciech Wiewiorówski (February 2021) *Opinion 2/2021 on the Proposal for a Digital Markets Act [PDF 143KB]*, EDPS (European Data Protection Supervisor), accessed 1 March 2021 [70].

37. If the ACCC continues to develop this proposal, consideration will need to be given to how these prohibitions would intersect with the Privacy Act and the proposed code for social media and online platforms which trade in personal information.[13]

The OAIC recommends:

- Proposal 2 be considered further, especially in relation to location information, and profiling, tracking or behavioural monitoring of, or directing targeted advertising at, children
- The ACCC consider the interaction between Proposal 2, the Privacy Act and other regulatory initiatives such as the Privacy Act Review and proposed code for social media and online platforms which trade in personal information.

Proposals 5 and 6 - Implementation of a common transaction ID and a common user ID to allow tracking of attribution activity in a way that protects consumers' privacy

38. These proposals consider creating a common user ID and transaction ID that will track users and transactions across the ad tech supply chain to assist industry participants in undertaking attribution and measuring the success of a campaign.

39. While acknowledging that these proposals are still being developed, the OAIC considers that there is potential for significant privacy risks to flow from the implementation of these reforms, particularly the common user ID.

40. The OAIC understands that the purpose of the common user ID is to allow multi-touch attribution to be conducted by all third-party attribution providers, addressing the imbalance between large platforms that have reliable user IDs and other attribute providers.

41. The OAIC also understands that multi-touch attribution will require tracking of consumers across devices and websites. This will be very privacy-invasive if the common user ID is or may become personal information. Technical information such as a common user ID may be personal information where it is about a reasonably identifiable individual, whether in isolation or when combined with other information held by (or accessible to) an entity. In the OAIC's view, as the ad tech industry incentivises the collection and linking of personal information, there appears to be a real risk that a common user ID could be personal information.

42. In relation to the common transaction ID, the OAIC understands that this will instead track transactions across the ad tech supply chain. Assuming the focus of this ID is on transaction data

[13] The Hon Christian Porter MP and Senator the Hon Mitch Fifield (24 March 2019) *Tougher penalties to keep Australians safe online* [media release], accessed 24 February 2021.

that is not linked to an individual consumer, this may carry a lesser risk of infringing on privacy rights. However, this proposal can only be adequately assessed once details of how the transaction ID will function, and what information will be transferred between ad tech participants, have been confirmed.

43. As noted above, the right to privacy is not absolute, however, privacy rights should only be limited where there is a compelling and substantial public interest reason to do so. In deciding whether to develop these proposals further, the ACCC should consider whether it is reasonable, necessary and proportionate, having regard to the potentially significant privacy risks that it creates.

44. The OAIC recommends that the ACCC undertake a PIA to determine whether the proposed common user ID and common transaction ID are reasonable, necessary and proportionate. The PIA should consider issues such as:

- The risk that a common user ID or common transaction ID are or may become personal information, and the extent that this can be managed or mitigated through the implementation of appropriate policies, procedures and privacy controls.
- The extent to which any other privacy risks and foreseeable future privacy risks stemming from these proposals can be managed or mitigated through the implementation of appropriate policies, procedures or privacy controls.
- Whether the objectives of these proposals can be achieved through other means that are less privacy intrusive.
- The parties that will have access to a common user ID or common transaction ID, and whether these parties are subject to the Privacy Act.

The OAIC recommends:

- The ACCC undertake a PIA to determine whether the proposed common user ID and common transaction ID are reasonable, necessary and proportionate. The PIA should consider issues such as:
  - The risk that a common user ID or common transaction ID are or may become personal information, and the extent that this can be managed or mitigated through the implementation of appropriate policies, procedures and privacy controls.
  - The extent to which any other privacy risks stemming from these proposals can be managed or mitigated through the implementation of appropriate policies, procedures or privacy controls.
  - Whether the objectives of these proposals can be achieved through other means that are less privacy intrusive.
  - The parties that will have access to a common user ID or common transaction ID, and whether these parties are subject to the Privacy Act.