Reset.
AUSTRALIA

Policy Submission

Submission to the ACCC AdTech Inquiry

Reset Australia would like to thank the Australian Competition and Consumer Commision (ACCC) for the opportunity to input into the Digital advertising services inquiry Interim Report. We commend the ACCC on the comprehensive report and its efforts so far in setting a high bar for countries around the world to begin to tackle the monopoly power of big tech and resulting consumer harms.

Reset Australia is an independent, non-partisan organisation committed to driving public policy advocacy, research, and civic engagement agendas to strengthen our democracy within the context of technology. We are the Australian affiliate of Reset, the global initiative working to counter digital threats to democracy. As the Australian partner in Reset's international network, we bring a diversity of new ideas home and provide Australian thought-leaders access to a global stage.

We look forward to working with the ACCC through this consultation and beyond, as we push this conversation forward to ensure appropriate and considered legislation that protects Australian institutions, citizens and democracy.

1. Context

Reset Australia acknowledges that the objectives or the inquiry are to address concerns related to the opacity in operation and pricing of ad tech services, as well as to promote competition in the ad tech industry, dominated by Google, while safeguarding user privacy.

With their multitude of consumer facing services and extensive network of trackers on third-party websites, Google has leveraged users' data across various lines of business to dominate other lines of business. This has blocked competitors, stifled innovation and ultimately reduced consumer choice.

This monopoly has been built by vacuuming up consumer data without the explicit consent of their users. Lengthy, all-or-nothing privacy policies have resulted in users having little understanding or control over how their personal data is being extracted and used.

Google has taken advantage of this opaqueness, intentionally collecting more data than necessary to deliver their services, with this 'surplus data' collection undetectable to their users. This has fed the development of detailed consumer data profiles used to sell their business customers targeted advertising. This economic model, coined 'surveillance capitalism' by Shoshanna Zuboff, was spearheaded by Google and sets a dangerous precedent for competitors, and flies against Australian ideals of autonomy, public safety and privacy.

Such data profiling has lead a range of consumer harms - from exclusion to price discrimination to inappropriate targeting. And the public is concerned, with 94% of Australian consumers uncomfortable with how their personal information is collected and shared online[1].

Like the ACCC, Reset Australia hopes for the outcome of the Digital ad services inquiry to be a more competitive ad tech industry. However, note that competitors should not be encouraged to build their services on the same extractive data practices that will continue to engender consumer harms.

2. Policy Approach

In order to protect consumers in the ad tech market, Reset Australia emphasises the need for a rights based approach to privacy, similar to that of the General Data Protection Act (GDPR) governing the EU and UK.

We acknowledge that the review of the Privacy Act 1988 is happening concurrently, and will inform the underlying privacy regulatory framework and the extent that users have control over their data. As noted in our submission to the review, an updated privacy act will serve to better future-proof this regulation in the face of a constantly changing digital landscape by setting a common reference point, and will mitigate some of the issues around ambiguity, broad interpretation and unclear compliance requirements[2].

While the ACCC have noted the Privacy Act review is outside of the scope of the ad tech services inquiry, certain core principles of Europe's privacy framework, the General Data Protection Regulation (GDPR) intersect with both the review of our privacy framework and the ad tech inquiry and if adopted would likely require consultation with the Office of the Australian Information Commissioner in the review of the Privacy Act.

- **Purpose limitation**[3] - Article 5(1)(b) says: "1. Personal data shall be: collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes."
    - The GDPR purpose limitation principle requires that personal data held by companies is ring-fenced and can't be used outside of consumer expectations.
    - Purpose limitation is being considered as is captured as a recommendation within Proposal 2: Data separation mechanisms.
    - Reset Australia supports purpose limitations, though note that in GDPR enforcement has been weak, so ensuring the ACCC is adequately set up to audit for compliance and have appropriate enforcement powers is necessary.

[1] 2020. New research finds Australian consumers want more control over their personal information and expect fair treatment. [online]
[2] Nyugen, M., 2021. Submission on the Review of the Privacy Act 1988 – Reset Australia. [online] Reset Australia. [online]
[3] Guide to the General Data Protection Regulation (GDPR), Principle (b): Purpose limitation. [online]

Reset Australia believes this should apply to not only companies operating in the ad tech industry, but to digital platforms more broadly. However note, this is may outside the scope of the inquiry and may sit within the Privacy Act review.
    - Further discussion in section 4b).

- **Data minimisation**[4] - Article 5(2)(c) says: 1. Personal data shall be: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)"
    - The GDPR data minimisation principle requires that data processes don't process and store more data than needed for the specific purpose
    - Data minimisation has not been captured as a consideration or potential recommendation in the Digital advertising services inquiry interim report, however we believe it should be considered as a measure to increase competition and consumer protections
    - Reset Australia supports data minimisation, noting that Google's monopoly has been built on the surplus of data that has been extracted in in the shadows and is beyond what consumers would likely consider a fair exchange
    - Further discussion in section 4b).

We agree with the ACCC that the regulatory burden should be proportionate to the market power and potential for consumer harm posed by the firm. We proposed a risk based approach, similar to that applied by GDPR where platforms that create the biggest risks, such as those processing sensitive category data (ethnicity, political or religious beliefs) or those processing personal data on a large scale would face the highest level of scrutiny. While those larger firms should face the heaviest burden, we urge that any laws that aim to protect consumer data are applicable to all ad tech companies.

In some instances, it may be appropriate certain requirements are applicable only for 'gatekeeper' organizations using unfair practices toward business users to gain a competitive advantage, as proposed in the European Digital Markets Act (DMA)[5]. Laws that promote competition through preventing self-preferencing could be made applicable only to those platforms deemed gatekeepers, allowing for competitors to innovate in the ad tech space without having to comply with unfair terms. This will allow business users who depend on gatekeepers access to a fairer business environment. See section 4c) for further discussion.

[4] Guide to the General Data Protection Regulation (GDPR), Principle (c): Data minimisation. [online]
[5] European Commission - European Commission. 2021. The Digital Services Act: ensuring a safe and accountable online environment. [online]

Responses to Proposals

3. a) Response to proposal 1: Measures to improve data portability and interoperability

We note the ACCC is considering data portability and interoperability as measures to reduce barriers to entry and expansion and promote competition in the supply of ad tech services, while ensuring consumers have sufficient control over the sharing and processing of their data.

Data portability is a positive mechanic to both promote competition and give users sufficient control over their data in the ad tech space. Such services would make transparent to consumers the extent of surplus data that digital services have collected on them without meaningful consent, empowering consumers to think about their data as a critical asset.

Data portability mechanisms should be developed in line with the Consumer Data Right (CDR)[6], ensuring accredited 3rd party recipients comply with privacy safeguards.

Recommendation: Proceed with data portability mechanic which enables users to have full control of the data they choose to move over to a 3rd party service. Develop inline with the Consumer Data Right (CDR) to ensure accredited 3rd party recipients comply with privacy safeguards.

Data interoperability is a concern due to the fact consumers lack agency in the transfer of data, which contradicts the ACCC's aim to ensure users have sufficient control. Due to this, we believe only very limited classes of data should be allowed to be transferred from one ad tech provider to another without explicit user consent. This should include data essential for attribution purposes only to address the opacity issues for publishers and advertisers, and should explicitly exclude any personal profiling data or data that could be used for re-identification. Profiling data has engendered a whole raft of consumer harms, and ad tech competitors should not be encouraged to be built on the same opaque, behind-the-scenes extractive data practices as that of Google.

Recommendation: Further clarify the asset classes which would be available for interoperability purpose, ensuring this includes only that which is essential for attribution purposes and excludes all consumer profiling data.

4. b) Response to proposal 2: Data separation mechanics

We note the ACCC is considering data separation mechanics such as data silos or purpose limitation requirements to level the playing field between large platforms and ad tech competitors.

[6] Office of the Australian Information Commissioner. What is the Consumer Data Right?. [online]

Google is currently operating in an internal data free-for-all whereby data from one area of the business is combined with data from another vertical, services and 3rd party tracking to give them a competitive advantage.

Reset Australia supports the ACCC's recommendation for mandated data silo rules prohibiting the sharing of data within such monopolies for the purposes of ad targeting. Such an approach may be necessary to address the instances where a consumer has no opportunity to interact with the user facing service to tailor their data preferences, as otherwise could be addressed by a purpose limitation requirement.

However, Reset Australia's preference is for a consumer-led approach to data separation, such as proposed as the purpose limitation requirement where consumers interacting with user facing services are given greater transparency and controls over the data collected. This would limit the collection of surplus data not necessary to deliver the consumer facing services, which has resulted in Google's outsized market power and a raft of consumer farms. Such an approach is in line with the 'purpose limitation' principle in the GDPR, as noted in section 3. Policy approach.

Recommendation: Implement a purpose limitation requirement for user facing services to be transparent as to the specific purposes for data collection. Offer users controls to opt-in and out of each specified purpose, prohibiting 'bundling' which forces users to opt-in to all or nothing agreements. Collaborate with the OAIC on the impact on the Privacy Act review.

It should be noted that the 'purpose limitation' principle is currently a requirement under the GDPR, however a lack of enforcement by the regulator has resulted in Google continuing to collect personal data with vaguely defined purposes that infringe on GDPR's purpose limitation. Brave browners Chief Policy & Industry Relations Officer Johnny Ryan has filed the complaint with Google's lead GDPR regulator in Europe[7], and has collated a table of instances demonstrating Google's data collection conflates multiple purposes[8].

To remedy this, there is an integral need for an audit authority to be instituted under the regulator, likely the ACCC. This would involve external risk auditing and data sharing with authorities and researchers to ensure compliance. Such models for oversight have been proposed in the EU Digital Services Act (DSA) and represent a clear pathway to emulate in Australia. Without mandated access, regulators are forced to rely on the companies to police themselves through ineffective codes of conduct.

Recommendation: Institute an audit authority under the regulator to ensure ad tech platforms comply with the purpose limitation principle and other principles implemented as

[7] Ryan, J., 2020. Formal GDPR complaint against Google's internal data free-for-all. [online]
[8] 2020. Inside the black box: a glimpse of Google's internal data free-for-all. [online]

a result of the ad tech inquiry. This should be coupled with high penalties for non-compliance.

The surplus level of user data collected by surveillance capitalists in excess of what users could predict, would consider a fair exchange, or is necessary to provide the specific service a user is accessing. This is both a competition issue and data protection issue.

Alongside the EU GDPR purpose limitation principle, is the data minimisation principle as noted in section 3: policy approach. This principle creates requirements for platforms to process and store the minimum level of personal data necessary for the specific purpose. Instating a similar data protection principle in Australia would not only increase competition and the level of consumer protection, but may also help to address consent fatigue, noted as a concern by the ACCC in a 'purpose limitation' approach. This is as it would reduce the number of purposes a service provider can collect data therefore instances for users to set privacy preferences.

Recommendation: Collaborate with the OAIC on the Privacy Act review to develop a data minimisation principle to address both competition and data protection issues.

Response to proposal 3: Rules to manage conflicts of interest and self-preferencing in the supply chain

We note that one remedy the ACCC is considering to reduce the ability of vertically integrated ad tech providers to engage in self preferencing is to requirements for increased transparency.

As a potential model, the Digital Markets Act (DMA) as referenced in section 3: Policy approach, establishes such obligations for 'gatekeeper' platforms - those who are vertically integrated and have an entrenched and durable position in the market. The DMA aims to ensure business users have access to a fairer market, increase the ability of competitors to innovate and enable consumers access to fairer prices.

Transparency obligations for gatekeepers in the DMA include providing advertisers and publishers with the tools and information necessary for carrying out their own independent verification of their advertisements. This will enable business users to better assess whether the platform is operating in their best interests and switch to alternate providers.

Recommendation: Implement transparency measures to mitigate self-preferencing in a model similar to Digital Markets Act, whereby the regulatory burden falls on gatekeepers whose vertical integration operations offer them a competitive advantage

Response to proposal 6: Implementation of a common user ID

We note the ACCC is considering a number of measures to address the lack of opacity and its impact on competition and efficiency in the ad tech supply chain.

Of concern the implementation of a common user ID to allow for tracking of attribution activity as it raises serious privacy risks. Assigning an ID to individuals will enable ad tech providers and advertisers to re-identify consumers against their existing customer base and as such result in further profiling of users of which they have not consented to. Such a measure would likely be strongly opposed by consumers, given their existing level of concerns about how their data is collected and shared online.

In addition, implementing a common user ID would also allow audience arbitrage, with low rent publishers (including disinformation publishers) enabled to sell the attention of a person who also is an audience member of a high end publisher. This audience arbitrage is explained in Dr Johnny Ryan of Brave's testimony at the International Grand Committee on Disinformation and "Fake News" in 2019[9]. Reference

"If you read about a luxury car on The Irish Times, and then later visit a less reputable website, you may see luxury car ads there. Companies that know you are a high value Irish Times reader – thanks to the Real Time BIdding system – show ads to you on the less reputable website at an enormous discount. They want you because you are an Irish Times reader, but The Irish Times does not benefit. The industry calls this "audience arbitrage".

Recommendation: We strongly oppose the implementation of a common user ID due to its privacy concerns, however also impress this will result in a negative impact for many publishers who will no longer able to monetise their audience

[9] Ryan, J., 2021. Ryan's testimony at International Grand Chamber: RTB data breach enables disinformation. Enforcers can be sued. [online]