8 August 2023

Digital Platforms Branch
Australian Competition & Consumer Commission
By email: digitalmonitoring@accc.gov.au

Ignoring privacy practices would distort data broker issues (Submission on Digital Platform Services Inquiry - March 2024 Report on Data Brokers - Issues Paper)

About us

Dr Katharine Kemp is Associate Professor of Law at UNSW Sydney and Deputy Director of the UNSW Allens Hub for Technology, Law & Innovation. Her research focuses on competition, consumer protection and data privacy regulation. She has published widely in these fields, including Misuse of Market Power: Rationale and Reform (Cambridge University Press, 2018) and Competition Law of South Africa (LexisNexis). Her advisory roles include representing Australia as a Non-Government Advisor to the International Competition Network and acting as a member of the Advisory Board of the Future of Finance Initiative in India, the Expert Panel of the Consumer Policy Research Centre, and the UNSW Data Protection Committee.

Graham Greenleaf AM is Professor of Law & Information Systems at UNSW Sydney. He has over forty years' experience as a privacy academic and advocate. Among his many privacy publications are Asian Data Privacy Laws (Oxford University Press, 2014) and Global Privacy Protection (Co-Edited with J Rule, Edward Elgar, 2008). He is Asia-Pacific Editor for Privacy Laws and Business International Report (UK). He is a member of the Council of Europe Convention 108 Consultative Committee and was an invited speaker at the European Union's launch of the GDPR. He has carried out numerous consultancy projects for the European Union and the Council of Europe on evaluations of data privacy laws in the Asia-Pacific.

The **UNSW Allens Hub for Technology, Law and Innovation** ('UNSW Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law and Justice, the Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the UNSW Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

About this Submission

We appreciate the invitation to make a submission on the "Digital Platform Services Inquiry – March 2024 Report on Data Brokers – Issues Paper" (**Issues Paper**). Our submission reflects our views as researchers; our views are not an institutional position. This submission can be made public.

This submission concerns data broker services that use information that relates to individuals and does not extend to services that use information that relates only to other matters such as data on businesses, traffic, or weather. We note that the focus of the Report will not extend to consumer and commercial credit reporting.

By way of summary, the main points in this submission include the following:

- To the extent that the Report is intended to present evidence on the state of competition in the relevant markets, the intended focus on "third-party data brokers" alone may preclude a full account of the competitive dynamics for at least some of the services in question.
- The most pressing problems raised by data broker services that use personal information are unlikely to relate to market power. Markets for the supply of such services are characterised by substantial negative externalities, especially having regard to their impacts on the data protection and privacy interests of individuals and society more broadly.
- These harms occur due to deficiencies in regulation and enforcement, including privacy and consumer protection regulation.
- Although these markets directly concern millions of Australians as individuals, these individuals are not participants in the relevant markets, and have no power or information with regard to the collection and use of their personal information.
- Mere increased transparency about complex data ecosystems – and unfair or unsafe data practices in those ecosystems – is not the solution.
- The ACCC should have regard to the full range of harms from data brokers' practices, including those which cannot be precisely discovered or quantified in economic terms.
- While we note that the ACCC has specified that this Report will not cover "the operation of Australian privacy laws", the likelihood of systemic breaches of the *Privacy Act 1988* (Cth) (***Privacy Act***) must not be ignored. Likely contraventions of Australian Privacy Principle 3.6 (**APP 3.6**), in particular, may not only harm individuals but greatly reduce the quality of services provided by data brokers to their business customers.
- Claims by data brokers that practices are "privacy safe" or "privacy compliant" or that data is "anonymised", "de-identified" or "not personal information" should be scrutinised as potentially misleading conduct under the Australian Consumer Law.
- It is critical that the privacy problems created by data brokers should not be reframed as a problem of "consumer education".

Market dynamics (questions 1-4)

The Issues Paper notes that the ACCC intends to focus only on "third-party data brokers" because the ACCC has previously examined the data practices of "first-party data brokers", and particularly the consumer data practices of digital platforms.

To the extent that the ACCC is considering the competitive dynamics of markets for certain products and services supplied by data brokers, it should be acknowledged that this focus on "third-party data brokers" alone will not take into account the full range of relevant competitive constraints. It is quite likely that services offered by firms outside the "third-party data broker" classification are substitutes for some of the relevant services. For example, it may be relevant that:

- third parties supplying additional personal information for individual customer profiles (without alerting the individual to this supply) include both data brokers supplying so-called "data enrichment" services and other digital platforms and retailers supplying personal information through "data matching" agreements;
- firms offering to relay advertisements or offers to groups of individuals or so-called "audiences" which are curated without choice or awareness on the part of the individuals[1] include both data brokers and major search, social media, news and entertainment platforms; and
- there are both data brokers and digital platforms offering "data analytics" services which may result in the collection of additional personal information in the form of inferences based on the analysis of existing personal information, without choice or awareness on the part of the individuals concerned.

Insofar as the Report is intended to present evidence on the state of competition in the relevant markets, the intended focus on "third-party data brokers" alone may therefore preclude a full account of the competitive dynamics for at least some of the services in question.

In our view, however, the most pressing issues created by data broker services are unlikely to stem from the exercise of market power, as explained in the following section.

Negative externalities and the role of individuals (questions 1-4)

Markets for the supply of data broker services that use personal information are characterised by substantial negative externalities, especially having regard to their impacts on the data protection and privacy interests of individuals and society more broadly. Data brokers do not need to possess substantial market power to create advantages for themselves at the expense of social welfare. These harms occur due to deficiencies in regulation and enforcement, including privacy and consumer protection regulation.[2]

[1] These individuals are generally grouped by the broker into so-called "audiences" based on a combination of attributes they supposedly possess, according to the design of the broker or the advertising customer. In most cases, the individual is not aware of their inclusion in this group, nor are they provided with notice about the attributes they are taken to possess or an opportunity to object to being included in the group.

[2] We have each addressed these deficiencies in, eg, Graham Greenleaf, 'Focus on the Key Reforms – Don't Be Distracted by the Rest (Submission to the Australian Federal Attorney-General on the Privacy Act Review Report)' (30 March 2023) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4404413> and Katharine Kemp, 'Unfair and Unsafe Data Privacy Practices of Popular Fertility Apps' (22 March 2023) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4396029>.

Increased competition does not cure negative externalities but has the potential to lead to a "race to the bottom" in the absence of adequate regulation.[3] Nor would it be sufficient to increase transparency about the practices of data brokers and their business customers for individuals, as explained below.

Although these markets directly concern millions of Australians as individuals, these individuals are not participants in the relevant markets. Individuals are not consumers of most of the services in question and individuals do not generally supply the data brokers with information. Some economists have attempted to conceive of individuals as suppliers of personal information as an input in these markets,[4] but this would be an entirely artificial characterisation when the individuals have no awareness of what information is being supplied to which data brokers with what consequences, let alone a choice about that supply. The existence of "take-it-or-leave-it" privacy terms buried in policies which permit no active choice about use of personal information for additional purposes does not constitute choice or consent by the individual.[5] Information about the lives of individuals is used by data brokers and their business customers for their own business purposes, without the involvement of the individuals.

However, mere increased transparency about complex data ecosystems – and unfair or unsafe data practices in those ecosystems – is not the solution.[6] Simply providing individuals with more information about the activities of data brokers will not lessen the harms caused by these activities any more than explaining methods of egg production to poultry will give caged chickens a better life.

Considering these market failures, the ACCC's examination of the services offered by data brokers and related data practices should be welcomed. The ACCC can play a vital role in extracting information about data practices that have remained opaque to individuals, civil society, and policymakers for too long and in illuminating the relevant market failures and consumer harms. This is likely to provide much-needed evidence as a first step towards appropriate enforcement and regulatory reform. However, to do this the ACCC must remain sensitive to the full range of privacy harms that are possible as a result of data broker activities.

Terminology (questions 1-4)

While it is important for the ACCC to understand the terminology used by data brokers to describe their products and services, the unquestioning adoption of that terminology should be avoided. Much of this terminology is created for the purpose of marketing data brokers' services and tends to obfuscate the true nature of the data practices.

---

[3] See Katharine Kemp, 'Concealed Data Practices and Competition Law: Why Privacy Matters' (2020) 16 *European Competition Journal* 628.

[4] See Shota Ichihashi, 'Non-competing data intermediaries' (Bank of Canada Staff Working Paper, 2020-28) <https://publications.gc.ca/collections/collection_2020/banque-bank-canada/FB3-5-2020-28-eng.pdf>

[5] See Graham Greenleaf, 'Focus on the Key Reforms – Don't Be Distracted by the Rest (Submission to the Australian Federal Attorney-General on the Privacy Act Review Report)' (30 March 2023), sections 11 and 12 on consent, privacy default settings, and 'fair and reasonable' practices'.

[6] See, eg, Matthew Crain, 'The Limits of Transparency: Data Brokers and Commodification' (City University of New York Academic Works, 2017).

For example, the term "audience" tends to suggest a self-selecting group of individuals who have consciously decided to observe a display of some kind. The data broker's "audience" is one constructed by third parties who decide that an individual is somehow similar to a group of other individuals based on information *and inferences* about their age, income, family situation, work, past searches, viewing and purchases, online interests, purchase intentions, and/or other behavioural data. These groups are often curated by firms with whom the individual has no contact, and the individual has no knowledge or choice about their inclusion in that curated group.

The word "audience" also connotes a group of people who are aware of a spectacle or activity provided by an "actor" (in the general sense). Here, the position is reversed: it is the actor (the data broker), by carrying out the activity of surveillance, who is aware of the details of all those under observation (the purported "audience") and not vice-versa.

The term "audience" is therefore a completely misleading term which should be avoided. It would be more accurate to refer to the individuals as "subjects" who are under observation, as in the subjects of an experiment.

Data brokers and their business customers also frequently refer to the role of these services in helping businesses to "understand" consumers and meet consumer preferences, suggesting communication and an alignment of interests with the consumer. This is marketing language intended to signal virtue, but it does not accurately represent the goals of the various actors. Data brokers are firms that have no connection with the individuals they report on but use information about those individuals' online and offline behaviour to promise businesses who may transact with those individuals a higher return on investment on their marketing campaigns or the ability to target "high value" customers. Despite several recent surveys on consumers' objections to the tracking of their online and offline activities and uses of that personal data for targeted advertising, data brokers and their customers seem uninterested in "understanding" these consumer preferences. In reality, what they seek to understand is how to extract greater consumer surplus. That goal may not be unlawful in itself, but it should not be disguised as a desire for "deeper understanding" of consumers in an attempt to improve the optics of the surveillance exercise.

Consumer harms (questions 16-23)

It is vital for the ACCC to have regard to the full range of harms from data brokers' practices, including those which cannot be precisely discovered or quantified in economic terms. The degradation of privacy is a significant harm even beyond any physical harm or financial disadvantage to an individual. Privacy harms also include humiliation, injury to feelings, "autonomy harms" (including undermining and inhibiting individual choice), increased susceptibility to future harm, and the loss of privacy as a social good.[7] This is not to suggest that competition and consumer regulation can be used to address every type of data protection or privacy harm, but that the ACCC should have regard to the full extent of negative externalities created by these markets in forming its views.

[7] See further Katharine Kemp and Melissa Camp, 'Pecuniary Penalties under the Privacy Act: Damage and Deterrence' in Deniz Kayis et al (eds), *The Law of Civil Penalties* (Federation Press, 2023) on the range and nature of privacy harms.

Privacy is a human right, which is vital to other human rights, including the right to dignity and the right to autonomy – and relatedly central to the development of personal identity, political freedom and consumer protection.[8] Therefore, the degradation of privacy cannot simply be weighed in the scales against economic efficiency gains for other actors.

Relevance of contraventions of the Privacy Act (questions 16-23)

While we note that the ACCC has specified that this Report will not cover "the operation of Australian privacy laws", the likelihood of systemic breaches of the *Privacy Act* must not be ignored. At the very least, it would be unsafe for the ACCC to recommend removing barriers to further collection, use and disclosure of personal information to level the competitive playing field, without having regard to the effectiveness (or lack of effectiveness) of privacy regulation in protecting the individuals concerned.

Potential unlawful conduct in the collection of personal information from third parties should be an area of particular concern. One of us has explained the likely unlawfulness of certain "data enrichment" practices in detail in a research paper,[9] concerning the obligations imposed by APP 3.6.

Data brokers have not explained how their conduct in collecting personal information from third parties – rather than directly from the individuals concerned – complies with APP 3.6. Nor have we seen any explanation of business customers' collection of personal information from the data brokers – rather than from the individuals concerned – complies with APP 3.6.

APP 3.6(b) provides that an APP entity must collect personal information from the individual unless it is unreasonable or impracticable to do so. Therefore, as a general rule, both data brokers and their business customers are obliged to seek personal information directly from the individual concerned. However, data brokers generally collect most personal information from sources other than the individual concerned. Further, data brokers provide "data enrichment" services that supply other firms with personal information – such as age, income, family situation, education level, purchase interests – which those firms could request directly from their own customers (permitting them an opportunity to refuse).

The OAIC guidance on APP 3.6 indicates that the mere fact that collecting personal information directly from the individual would be "inconvenient, time-consuming or impose some cost" does not make it unreasonable or impracticable.[10] While third-party data brokers may have no existing relationship with the individuals profiled by their data practices, it would be absurd to argue that the lack of any proximity to the individual exempts an APP entity from compliance with the direct

[8] See N Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford University Press, 2015) 412–421.

[9] Katharine Kemp, 'Australia's Forgotten Privacy Principle: Why Common 'Enrichment' of Customer Data for Profiling and Targeting is Unlawful' (Research Paper, 27 September 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4224653>

[10] OAIC, 'Australian Privacy Principles Guidelines', para 3.65 <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information#collecting-directly-from-the-individual>

collection rule in APP 3.6. It is also important to note that individual consent alone is not an exception to the direct collection rule.

Although recommendations regarding changes to the *Privacy Act* may be beyond the scope of this report, in our view, the ACCC can and must remain sensitive to data broker practices that are potentially in breach of the Privacy Act. To do otherwise would restrict its recommendations to those based on an artificial view of reality.

Scrutiny under the Australian Consumer Law (questions 16-19)

Claims by data brokers that practices are "privacy safe" or "privacy compliant" are intended mollify business customers who may have compliance or reputational concerns, but they are almost never supported by any adequate explanation as to how the practice complies with privacy laws or protects individuals' privacy. Such claims should be scrutinised under the Australian Consumer Law as potentially misleading conduct or false representations.

There should also be scrutiny of representations made to consumers or business customers that data is "de-identified", "anonymised" or "not information that personally identifies you". These representations may indicate that the firm considers the information to fall outside the scope of the *Privacy Act* and/or create the impression that this data does not affect the privacy of individual consumers. However, there is a growing range of data services that affect the privacy of individuals while claiming not to use personal information, including the creation of persistent unique identifiers, data "matching" or "enrichment" using hashed emails, and other "identity resolution" services. Obfuscation about such activities may not only mislead consumers, but hinder competition on privacy quality by firms that seek to compete on the basis of genuinely privacy-enhancing features.[11]

Quality of services offered to business customers (questions 4, 16)

The legality of data practices under the *Privacy Act* is also relevant to the quality of services offered by data brokers. Services based on, or leading to, contraventions of privacy law are poor quality services for data broker customers. If, for example, purchasing a data broker's "data enrichment" services constitutes a breach of APP 3.6(b) by the business customer on the basis that the information provided is in fact "personal information" under the *Privacy Act* (and the purchaser could reasonably request it from the consumer themselves), the data broker is offering a poor quality service for any business customer seeking to comply with the law.

Information asymmetries and lack of transparency (questions 20, 21, 23)

Privacy policies presented to consumers are notorious for their vague, broad terms and use of ambiguous and confusing language. In the context of data brokers' services, there are additional issues in respect of information asymmetries and lack of transparency regarding data practices:

[11] Explained further in Katharine Kemp, '"A Rose by Any Other Unique Identifier": Regulating Consumer Data Tracking and Anonymisation Claims' (August 2022) *Competition Policy International TechReg Chronicle* 21 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4248453>.

- Most consumers have no knowledge of which data brokers use their personal information and therefore no access to the relevant privacy terms, even if those terms were to provide useful information;
- To the extent that consumers supposedly consent to the disclosure of their personal information to or by data brokers based on the privacy policies of retailers, digital platforms or customer loyalty programs with whom the individual interacts, the terms of these privacy policies tend to be so broad and vague that the individual receives no real notice or choice in the matter, and would be unlikely to understand how these policies refer to data brokers;[12] and
- Privacy terms and marketing used by data brokers, their "data partners" and business customers sometimes include inaccurate or ambiguous representations about the allegedly non-personal nature of the information in question, for example, through claims that information is "de-identified", "anonymised" or "not personal information".

While the Issues Paper specifically asks consumers whether they have experienced any harm as a result of a product or service provided by a data broker, it would be very rare for consumers to be able to identify a data broker as the source of any harm they have suffered. For example, a consumer is highly unlikely to discover that they have been excluded from a particular offer on the basis that a data broker has allocated them to a certain "audience" or otherwise indicated that the individual has certain attributes.

Consumer education is not the answer (question 22)

Question 22 of the Issues Paper asks about which "bodies or resources exist to assist and support consumers in their dealings with data brokers" and "[w]hat more could be done to better educate and empower consumers". Consumers do not tend to have any dealings with data brokers because they have no information about which of the many data brokers hold data about them or what that data is.[13] Nor could consumers fairly be expected to deal with the many data brokers who might hold data about them.

It is critical that the privacy problems created by data brokers should not be reframed as a problem of "consumer education". Even if data brokers were entirely open with consumers about what data they hold on them, where they obtained it and who they disclose it to for their business purposes, this would not make those data practices fair or reasonable. This is not a matter of educating consumers or, still worse, explaining any disingenuous "value proposition" to them. The data practices we have explained in this submission are unfair and harmful and should be stopped.

Katharine Kemp and Graham Greenleaf, 8 August 2023

[12] This is especially the case where privacy policies only refer to "third parties", "trusted partners" or "data partners" to the extent that any description of a third party in the policy could be taken to include data brokers.

[13] As noted, credit reporting services are not included in the services under examination.