Comments on ACCC Issues Paper - Digital Platform Services Inquiry – March 2024 report on data brokers

22 September 2023

Peter Leonard
Principal, Data Synergies
Professor of Practice, UNSW Business School

Data Synergies (Peter Leonard)[1] - Comments on ACCC Issues Paper - Digital Platform Services Inquiry – March 2024 report on data brokers[2]

The following comments respond to the ACCC's invitation for interested parties, as informed by the Commission's Issues Paper of 10 July 2023, to make written submissions to assist the ACCC in understanding the nature of the data broker industry in Australia and any related competition and consumer issues that may arise.

There are three key problems in discussing the "the data broker industry", which coalesce into a central issue: there is no logical coherence for policy development across the diverse business activities and associated data practices discussed in the Issues Paper as data broker activities.

1. Over-inclusiveness

The ACCC's characterisation of "data brokers" and "the data broking industry" as including any first party or third party entity that shares "personal information and other information on persons" with other entities is overly broad. It brings within scope diverse businesses and myriad business practices:

- that are not considered data broker activities in any comparable jurisdiction,
- which do not create significant risks of consumer harms, including any of the recognised categories of privacy harms, beyond those risks of harms addressed through operation of provisions of Australian Consumer Law, as proposed to be supplemented by amendments to address unfair business practices, and
- which do not create significant risks of recognised categories of privacy harms, beyond those risks of harms addressed through operation of provisions of the Privacy Act 1988, as proposed to be supplemented by amendments canvassed in the Australian Attorney-General's Department's Privacy Act Review.

Over-inclusiveness in scope carries a risk of insufficient focus upon more limited categories of data sharing for reward that manifestly carry significant risks of consumer harms. These risks of harms commonly arise because many individual entities implementing relevant business models and associated data practices do not appropriately assess and mitigate risks associated with under-controlled data sharing. This failure in data governance and assurance is in many cases attributable to:

- shortcomings in business processes of the data collecting entity,

[1] Peter Leonard is a business consultant and lawyer advising data-driven businesses and government agencies. Peter is principal of Data Synergies and a Professor of Practice at UNSW Business School (Information Systems and Technology Management, and Management and Governance). Peter serves on the NSW Government's AI Review Committee and the NSW Government's Information and Privacy Advisory Committee, and a number of corporate and advisory boards. He is immediate past chair of the AI Ethics Technical Committee of the Australian Computer Society and the Privacy and Data Committee of the Law Society of New South Wales.

[2] https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry%20-%20March%202024%20report%20-%20Issues%20paper.pdf

- shortcomings in business processes of the data receiving entity (in relation to its own activities, or those of further downstream data receiving entities), and
- sometimes both.

Less commonly, the risk of harms is inherent to, and a necessary feature of, the business practice itself: the characterisation of these business practices is further discussed below.

Over-inclusiveness also risks placing Australian regulation substantially out of step with developing regulatory norms and evolving regulatory best practice in comparable jurisdictions.

2. Currently moving adjacencies

The ACCC's review is taking place concurrently with the Australian Attorney-General's Department's Privacy Act Review. As the ACCC is aware, the A-G's review includes consideration of proposals to amend the Privacy Act to address significant risks of consumer harms associated with certain data sharing business models - in particular, 'trading' (as it should be defined) 'in personal information' and highly targeted online advertising[3] - and associated data practices which manifestly carry significant risks of consumer harms. The appropriate scoping of proposals for privacy law reform is discussed further below.

This submitter is on the view that:

- recognised categories of privacy harms to individuals[4] should be addressed by appropriately scoped changes to the Privacy Act 1988 (C'th), and allocation of further enforcement resources to the OAIC,

[3] See further comments on Proposal 20.1, at pp42-46, in Data Synergies (Peter Leonard), 'Comments on Proposals in Privacy Act Review Report', Submission in response to Australian Attorney-General's Department's Privacy Act Review – Report, February 2023. The submission is published at https://consultations.ag.gov.au/integrity/privacy-act-review-report/consultation/download_public_attachment?sqId=pasted-question-1676440442.95-78210-1676440443.24-67813&uuId=99378981

[4] Examples of privacy harms include inconvenience or expenditure of time; a negative outcome or decision with respect to an individual's eligibility for a right, privilege, or benefit, such as related to employment, credit, insurance, government assistance, certification or licences, including denial of an application, obtaining less favourable terms, cancellation, or an unfavourable change in terms; online abuse; undue discrimination; stigmatisation or reputational injury; disruption and intrusion from unwanted communications or contacts; and other detrimental or negative consequences that affect an individual's private life, privacy affairs, private family matters or similar concerns. Assessment of risk of harms also requires consideration of balancing actors, including whether any significant effect upon an affected individual is reasonably likely to be likely to be understood by an affected individual, whether the act or practice is transparent to an affected individual, whether the affected individual has provided unambiguous affirmative consent to the particular acts or practice, whether the act or practice is beneficial to an affected individual, whether the act or practice provides societal benefits or creates or contributes to societal detriments such as erosion of trust of citizens in use of digital services or compromise of digital identity or data security, whether the act or practice is consistent with the context of the relationship between the individual and the entity, whether the act or practice is in fulfilment of a legitimate business purpose and the effect of the act or practice is necessary and proportionate to fulfilment of that legitimate business purpose, whether the entity has established, implemented, tested, revised, and documented reasonable and appropriate policies, procedures, and technical controls and safeguards, taking into account the purpose of the act or practice and the level of risk, and the effect of technical, operational, legal and other controls and safeguards, taken as a whole, to mitigate risk of privacy harms arising from the act or practice and to manage residual risks which cannot reasonably be mitigated. See further Data Synergies (Peter Leonard), Privacy Harms: A research paper for the Office of the Australian Information Commissioner, June 2020, https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/research-publications-on-the-privacy-act; Danielle Keats Citron and Daniel J Solove, 'Privacy Harms', 102 Boston University Law Review 793 (2022), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222.

- the ACCC's review should take cognizance of the regulatory changes that are outside the ACCC's regulatory purview but are currently in train to address misinformation and disinformation, online safety, information security, and harms more directly associated with AI and algorithmically enabled automated decision-making.

Many assertions of civil society organisations as to possible harms associated with 'data broker activities' do not take cognizance of these changes.

This review should focus upon gaps in coverage of existing provisions of Australian Consumer Law and competition provisions of the Competition and Consumer Act, as applied to activities reasonably considered to be data broker business practices.

3. What should be a relevant data broking activity?

Care needs to be taken in characterisation of which acts and practices associated with sharing of data are properly regarded as a data broking activity, in contradistinction to myriad other data sharing acts and practices that enable organisational activities today.

In undertaking that characterisation, three areas should be evaluated:

- **inputs**: the nature of the data (**ingress data**) received by the entity (said to be a data broker),
- **data context (i.e., controlled data environment)**: the environment in which data is handled by the entity, including technical, operational, organisational and legal (including contractual) guardrails, safeguards and controls of data while in a controlled data environment isolated from other data environments under the control of the entity, and absence or reasonably foreseeable ineffectiveness of that data governance and assurance,
- **outputs**: outputs as used or released by that entity (**release data**), including radically transformed outputs such as aggregated insights. This evaluation should include consideration of the purposes for which those outputs are intended to be used, or might be used, as a reasonably foreseeable consequence of the releasing entity making available release data outside of its effective control and without, or with ineffective, safeguards or controls.

Many business processes of most organisations (including government agencies such as the ACCC, not-for-profits and businesses) involve some data sharing with third parties to enable the first party organisation to undertake its activities. Use of applications-as-a-service, and associated sharing of data in multiparty data ecosystems, are the norm and an essential incident of the modern Australian economy.

By way of some examples, there does not appear to be a policy justification to characterise as a "data broking activity" provision or use of Microsoft365, Adobe Suite services, payments platforms, Xero or MYOB, or Salesforce and the many CRM applications available on the Salesforce platform. This observation applies regardless of the fact that providers of each of these applications-as-a-service make varying secondary uses of information and insights derived from "information on persons" as

'shared' by customers with the provider in the course of those customers' use of the provider's applications.

A significant subset of data sharing business activities are practices that facilitate third party data analytics service providers to provide business enhancement services such as production, distribution and other supply chain optimisation, reduction in wastage and returns, better allocation of products across distribution centres or outlets, development of broadcast marketing or advertising campaigns, and better forecasting of patterns of demand for particular products or services. There does not appear to be a policy justification to characterise any of these activities as a "data broking activity". In each case, there is a use of "information on persons", but not in a manner or for a purpose that is directly related to the entity's manner of dealing with those persons, such as differential treatment of those persons.

Two further, and mutually overlapping, subsets of data sharing business activities are acts or practices of using "personal information" (relating to identifiable individuals), or "information on persons", or both:

- to determine whether, how, and subject to what conditions, to offer products or services to persons within the relevant data sets, either as an audience segment, or in more granular cohorts, or individually, and
- for targeted advertising.

Some adtech service providers and other intermediaries working within the multiparty data sharing flows associated with digital advertising practices implement data use case business models of for-reward (including reward through derivation of contra and other business benefits) provision of information about persons in a data context where the release data (1) enables a recipient of that release data to identify people within that data set, and thereby (2) facilitates a recipient using that information to affect whether, how, and subject to what conditions, that recipient (or any downstream entry from that recipient) deals with people within that data set. Such activities might reasonably be characterised as "data broking".

However, if the same "information on persons" data set was used for the same purpose but entirely within the operations of a first party (including through the assistance of a data processor acting under the effective control of the first party) and without relevant "information on persons" data leaving that sphere of control, this activity should not reasonably be characterised as "data broking": there is no relevant trading in the relevant data.

Comparable jurisdictions that specifically regulate activities of data brokers[5] do not extend that regulation beyond (1) sharing between entities of personal information for the purpose of targeted advertising, and (2) sharing between entities of personal information for other purposes and in data contexts where personal information leaves the sphere of control of the disclosing party. Comparable jurisdictions that have regulated data brokers, or recently reviewed whether regulation of data

[5] For a recent comparative review of data broker regulation in the U.S.A., see Jessica Rich, 'Mounting Focus on Data Brokers: Is More Regulation Coming?', 24 August 2023, https://www.kelleydrye.com/viewpoints/blogs/ad-law-access/mounting-focus-on-data-brokers-is-more-regulation-coming

brokers may be justified, have focussed upon acts or practices where the third party receives and handles information about individuals that are reasonably identifiable in the hands of the receiving party or another entity downstream of the receiving party.[6] To state the same proposition a different way, a recipient's capability (whether or not exercised) to identify, or re-identify, particular persons within a dataset is an essential element or characteristic of a "data broker" "activity" as regulated, or currently under consideration for regulation, in comparable jurisdictions. It is not clear why the ACCC considers that Australia might need to uniquely take a different approach. In the Issues Paper "data broking" is used to encompass for-reward sharing of:

- "personal information", being information that (to adopt the clarifications of current law as proposed for the Privacy Act reforms) relates to individuals who are reasonably identifiable in the hands of the receiving party or any other downstream entity (also having regard to other information available to that receiving party or other downstream entity), and
- "other information on persons", regardless of whether those persons are identified, or reasonably identifiable, in the hands of the receiving party or downstream entity.

This breadth of characterisation thereby captures, as a data broker activity, myriad forms of information sharing without regard to operation of demonstrably effective privacy protections: that is, protections through implementation and reliable operation of technical, operational, organisational and legal (including contractual) safeguards and associated controls against reidentification. Emerging good practice in multiparty data ecosystem governance includes substitution of one-way hashed transaction or transactor keys or codes for stripped direct and indirect identifiers (before the data is shared in the form of ingress data), data treatment to strip sensitive or higher risk data points which might be used to effect data harms on data subjects, implementation of controlled data analytics environments (i.e., data clean rooms), and use of privacy protective technologies and data handling practices.

Where data governance and assurance measures are implemented in a manner which is objectively assessed as verifiably reliable to protect persons (being the subjects of the "information on persons") from being reasonably identifiable, query whether the act or practice should be construed as a "data broker activity".

[6] By way of example, on 14 September 2023, the California legislature passed S.B. 362, a bill that would impose new requirements on data brokers and grant residents new rights designed to facilitate control over their personal information. S.B. 362 is now pending assent by the California Governor. The Act aims to close a loophole in the California Consumer Privacy Act (CCPA) that allows consumers to request that data brokers delete personal information obtained directly from the consumer, but does not require data brokers to delete personal information obtained from other sources. The Act does not amend the existing definition of "personal information" in the CCPA, which is "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." That definition also expressly excludes publicly available information, meaning information that is available from federal, state, or local government records, and pseudonymised and de-identified information or aggregated and de-identified information that cannot be reasonably be linked to an individual. The Act defines the term "data broker" broadly to include any business that "knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." The Act will require data brokers to register with the California Privacy Protection Agency (CPPA), pay a fee, comply with disclosure and recordkeeping obligations, direct the CPPA to create an accessible deletion mechanism that allows consumers to exercise deletion requests simultaneously with regards to multiple data brokers, require data brokers to continue to delete any new information received about the consumer every 45 days, and require data brokers to undergo independent compliance audits every three years. The Act is available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB362.

Further, “information on persons” potentially includes transformed data in the form of aggregated insights or otherwise shared in a form that does not relate to individual persons within the cohort that constitutes the aggregation: the ACCC’s use of “on persons” is not qualified to relate only to transactor level persons (i.e., unique individuals, who may not be identifiable). There appears no compelling justification to bring within policy scope the common practice of deidentified data sharing to facilitate creation of aggregated insights. Indeed, many public health and other public policy and business improvement initiatives are built upon such data sharing.

4. Focussing upon areas of expressed concerns

Query whether the policy scope for data brokers might include the limited use case where the business model is a receiving (third) party that creates aggregated insights providing a service to the first party (data collector) of provision of insights in the form of so-called customer behavioural factors (CBFs) (viz., algorithmic inferences about a person’s characteristics, preferences or interests) for the purpose of the first party using those CBFs for differentiated treatment of individuals within the cohort.

One view is that this data augmentation activity is relevantly of the first party and that, by the act or practice of linking the customer behavioural factors with personal information held by that first party, this third party should be regulated (to the extent that regulation is justified) by the data privacy statute in relation to such activity. On this view, there is not a compelling policy need to also regulate the provider of those insights.

A further area for consideration is the purpose for which release data (outputs) are intended to be used by a recipient entity, or might be used as a reasonably foreseeable consequence of a releasing entity making available release data outside of the entity’s effective control in absence of, or with ineffective, safeguards or controls. This is where the ACCC in the course of this review may need to engage with an emerging academic debate about ‘personalisation’, ‘individuation’ and other forms of ‘consumer profiling’.

Some academics and privacy advocates assert that an act or practice of an entity enabled by use of information about a person (regardless of whether identifiable) that enables that person to be treated differently from another person should be regulated by provisions of the data privacy statute as a use of personal information about that individual, regardless of whether actual mechanism for the differential treatment itself involves a use of information relating to an individual that is identifying of that individual.

Generally this assertion is made in relation to non-contextual targeted advertising, although sometimes the assertion is sometimes also made in relation to a broad range of other business models of data-analytics enabled differentiation between persons. This assertion therefore is an extension of the view that targeted advertising should be regulated by the Privacy Act 1988, even in data situations where targeted advertising is enabled by use of data clean rooms and privacy enhancing technologies that have been objectively assessed as reliably effective to mitigate risks of identification of relevant internet users, and risks of impermissible uses and disclosures of relevant data.

Although the underlying legal reasoning is commonly not articulated by the proponents, the proposition appears to be that if (both) (1) personal information was used to create ingress data, and (2) an ultimate outcome is differential treatment of persons, then (the proponents assert) it should be irrelevant whether the data analytics environment (data context) and outputs (release data) assure that no identifying information is used or released (disclosed). In other words, the proposition appears to be that existence of a causal chain linking (1) use of "personal information" to create ingress data (even where that ingress data is not of itself "personal information"[7]), and (2) the outcome of differential treatment, is not broken by intermediate steps that assure that there is no use or disclosure of "personal information" either as defined in current provisions of the Privacy Act 1988, or as proposed to be amended.[8] In the writer's understanding, the assertion appears only to be made where manifestly "personal information" is used to create ingress data, although it should be noted that there are many use cases where information that is not personal information, but which enables uniqueness of a person to be established, may be (and commonly is already) used to create ingress data that is causally linked to differential treatment of that person.

The policy rationale for the proposition is sometimes stated as that there should be transparency to the affected person as to why and how they are being the subject of differential treatment, and the possibility of opt-out from differentiated treatment. The writer's perspective is that it is not clear why this particular form of differentiation between affected persons, in contradistinction to the myriad other was in which businesses differentiate between persons in both online and offline interactions with consumers and other users, should be the subject of further regulation. Differential treatment is enabled by many inferences made by humans or machines about humans about observed behaviour of other humans: it is not clear why this particular form of observation should be regulated above more general regulation of differentiated treatment of consumers (broadly defined) through economy wide restrictions as to differentiated effects under anti-discrimination and consumer law statutes, and e-safety rules (including as to geo-tracking) to protect children and other vulnerable groups.

5. Data broker activity and targeting

Where information is pervasively deidentified by aggregation, it should not be regulated as personal information, and subsequent uses and disclosures of that information should not be regarded as data broking activities.

Release of effectively anonymised information may, or may not, be a disclosure of personal information by the holder of that information, depending upon the context of the release environment and the attendant risk of identification or reidentification in that release environment, as above discussed.

[7] Where the ingress data is personal information, the collection and handling (including associated data linkages and joining) of that ingress data will be regulated acts and practices in relation to personal information regulated by existing provisions of the Privacy Act 1988.
[8] The effect of the current proposals is discussed by the author in Data Synergies (Peter Leonard), 'Comments on Proposals in Privacy Act Review Report', Submission in response to Australian Attorney-General's Department's Privacy Act Review – Report, February 2023. See, in particular, comments on Proposals 4.5 and 4.6, at pp 9-10; and Proposal 20.1, at pp 42-46. The submission is published at https://consultations.ag.gov.au/integrity/privacy-act-review-report/consultation/download_public_attachment?sqId=pasted-question-1676440442.95-78210-1676440443.24-67813&uuId=99378981

If an entity holding effectively anonymised information elects to release that information from a particular data content into a different context (whether controlled by that entity, or by another entity) in a form where there is a reasonable likelihood that the recipient may append that information to profiles or other information relating to individuals that are identified or reasonably identifiable, or otherwise identify the individual, there is a policy justification to consider this act a regulated disclosure of personal information by the discloser, even though the relevant information was not regulated personal information in the hands of the disclosure (before the point of disclosure). This activity might also be reasonably characterised as a 'data broker activity'.

The primary mode of regulation of sharing of personal information between entities (that are not related bodies corporate) should be the operation of the APPs in the Privacy Act addressing disclosure of personal information and in particular requirements that the disclosure:

- is for a clearly and prominently described purpose,
- is necessary and proportionate to effect that described purpose,
- is reasonable,
- if a disclosure of a defined category of sensitive information, requires consent.

Consent should not operate as a qualification to the other requirements. Consent by itself is an inappropriate tool to regulate trading in personal information as broadly defined because:

- individuals should not be expected to evaluate whether the other requirements have been fulfilled,
- there are common misunderstandings as to the ways in which information can be shared between APP entities to facilitate a particular transaction or interaction without any disclosure of personal information by an APP entity, and without the recipient entity receiving information in a form which is personally identifying in the hands of the recipient or that may be used or further disclosed by the recipient as personal information,
- addressing those common misunderstandings would often require engaging with individuals about complex technical processes and technical, operational and legal safeguards and controls to ensure that there is not disclosure of personal information, when that engagement should not be necessary if to the other requirements have been fulfilled.

Diverse multiparty data ecosystems and data flows between entities are a reasonable and necessary incident of a vibrant digital economy. Overly restrictive regulation of multiparty data ecosystems and data flows between entities principally advantages those relatively few large business entities and government agencies that can conduct their operations without substantial data sharing. Some data sharing – for example, between loyalty partners and a scheme operator to facilitate operation of customer loyalty programs - is an essential element of conduct of an entity's business.

A small subset of data flows between entities in multiparty data ecosystems may fairly be characterised as trading in personal information and thereby justify additional regulation.

A clear example is disclosure of personal information through provision of customer lists or access to customer databases where the provider receives financial reward or comparable benefit or advantage that is reasonably attributable to that disclosure of personal information. This is an example of a 'data brokerage' activity that should be regulated as a disclosure of personal information, and also (and further) regulated by a requirement for consent of an affected individuals, because:

- many citizens consider that is of a level of privacy intrusion, or derivation of value from use of information about their attributes or activities without value delivered to them as affected individuals, that is unacceptable, and
- the risk of harms to affected individuals caused by a recipient that is not in a direct contractual or other transactional relationship with the affected are unacceptably high, noting that the recipient will as a result of the transaction have access to and use of personally identifying information relating to the affected individual that is controlled only by the general requirements of the APPs as apply directly to the recipient entity.

Regulation of trading in personal information as a data broker activity should be clearly delineated to address this small subset of activities of disclosure of personal information.

Peter Leonard,
Principal, Data Synergies and Professor of Practice, UNSW Business School
22 September 2023