Consumer Policy Research Centre

Submission

Data brokers – Australian Competition and Consumer Commission

16 August 2023

About the Consumer Policy Research Centre

The Consumer Policy Research Centre (CPRC) is a not-for-profit consumer policy think tank.

Our work is possible thanks to funding from the Victorian Government.

Our role is to investigate the impacts that markets and policies have on Australian consumers and advise on best practice solutions. Consumer protections in the digital world is a current research focus for CPRC.

Contact for submission

Chandni Gupta
Deputy Chief Executive Officer + Digital Policy Director

Email: chandni.gupta@cprc.org.au

Submission made via: digitalmonitoring@accc.gov.au

Statement of Recognition

CPRC acknowledges the Traditional Custodians of the lands and waters throughout Australia. We pay our respect to Elders, past, present and emerging, acknowledging their continuing relationship to land and the ongoing living cultures of Aboriginal and Torres Strait Islander Peoples across Australia.

You cannot challenge what you don't know

Data brokers operate as modern-day alchemists of the data world. **They are mining and refining consumer data and then sharing and selling it to the highest bidder.** Insights from data broker services can support businesses to refine their advertising targeting strategies which can be anything from personalising what products consumers may be offered, what prices they pay or whether they are excluded from specific products and services.

There is little to no transparency in how data brokers collect, share and use personal information. This presents three key risks for Australian consumers:

1. It's unlikely that consumers even know that their data is being collected by a data broker.
2. It is highly unlikely that consumers have given explicit consent for that collection.
3. There is no clear way to opt-out of having your data collected in the first place.

As for many data-based related practices, the issue cannot be resolved in a piecemeal approach. The Federal Government must prioritise the following economy-wide reforms to deliver a holistic consumer protection framework that effectively holds data-enabled businesses accountable:

- Introduce an unfair trading prohibition to protect consumers from businesses that unfairly exploit their customers.
- Reform the Privacy Act to bring Australia's protection framework into the digital age.
- Implement a best-interests duty or duty of care obligations for data.

At a minimum, the Federal Government should consider labelling requirements for products and services where data captured or used involves data brokers. In addition, the ACCC should consider using its information gathering powers to identify the prevalence and process of consumers requesting information or redress from data brokers.

Our submission uses insights from CPRC's research and considers the questions raised in the issues paper using three key principles – fairness, safety and inclusivity for consumers engaging in the digital economy.

We would welcome the opportunity to work with the ACCC and share further insights from our consumer research projects. For further discussion regarding our research and the contents of this submission, please contact chandni.gupta@cprc.org.au.

Question 17: What consumer harms may arise from the collection, processing, analysis or storage of information by data brokers? Which consumers are most likely to be harmed and why?

Question 18: What consumer harms may arise from the use of data products and services sold or provided by data brokers? Which consumers are most likely to be harmed and why?

There are four tiers of harms that consumers risk facing from the collection, processing and analysis, storage and use of information by data brokers:

- **Manipulation**: sophisticated companies can have the power to design online user interfaces in very manipulative ways, for example, by using dark patterns.[1] Companies can use the insights they've acquired through data brokers about customers to shape what products are shown and what information is presented, effectively exacerbating the information asymmetries between companies and consumers. Manipulation can also lead to unfair outcomes, misuse of data, compromise the dignity of consumers and hinder or distort competition.[2] CPRC's research into dark patterns revealed that manipulative online design is costing Australians money, is leading to a loss of control over their personal information and impacting their wellbeing – 83% of Australians have experienced negative consequences as a result of dark patterns.[3]

  Example: CPRC's previous data research identified that Quantium was using de-identified transaction data from the National Australia Bank which was supporting advertising for Sportsbet. The line can be clearly drawn between data broker practices and how easily it can lead to exploiting people's vulnerabilities for profit.[4]

- **Discrimination and exclusion**: also known as digital red-lining, insights curated through data brokers about consumers can be used to benefit commercial entities in discriminatory ways that is at direct odds with the needs and interests of consumers.[5] For example, data can be used to build an "online profile" of a consumer and effectively "score" their value – with a view to identifying and retaining profitable customers through advertisements (and avoiding those who are not profitable).[6] A lack of transparency and accountability within such processes means it is difficult for consumers to see how their profile is produced; understand the impact it will have on them; or influence, appeal or correct assumptions based on wrong information.[7] Profiles can also be used to set prices, leading to some groups of consumers paying more for the same service.

  ***Example*:** In 2020, a CHOICE investigation into personalised pricing found that people over the age of 30 were offered prices more than double the prices of those aged under 30 on the dating app, Tinder. While it is not a direct example of use of data brokers, it highlights the issue of how targeted profiling can lead to discriminatory and exclusionary practices.[8]

- **Lack of control:** CPRC consumer research indicates consumers are uncomfortable with the amount of information collected about them and would prefer to have greater control over that data collection.[9]

[1] "Dark Patterns" that make it difficult for users to express their actual preferences or that manipulate users into taking actions that do not comport with their preferences or expectations. For more information see the Stigler Centre's 2019 Committee on Digital Platforms – Final Report (p. 12).
[2] Kayleen Manwaring, "Will emerging technologies outpace consumer protection law? The case of digital consumer manipulation", (2017), *Competition & Consumer Law Journal*, 26, 149, https://www.accc.gov.au/system/files/Kayleen%20Manwaring%20%28December%202018%29.PDF.
[3] CPRC, "Duped by design - Manipulative online design: Dark patterns in Australia", (June 2022), https://cprc.org.au/dupedbydesign/.
[4] Brigid Richmond, "A day in the life of data", (2019), https://cprc.org.au/research-report-a-day-in-the-life-of-data/.
[5] University of Melbourne, *State of the Art in Data Tracking Technology,* 2019, p. 14.
[6] Wolfie Christl, "Corporate Surveillance in Everyday Life", (June 2017), Cracked Labs, p. 13, https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf.
[7] Cathy O'Neil, "Weapons of Math Destruction", (2016), Crown Books, p. 143.
[8] See CHOICE's investigation into Tinder: https://www.choice.com.au/about-us/media-releases/2020/august/tinders-secret-pricing-practices.
[9] CPRC, "CPRC 2020 Data and Technology Consumer Survey", (December 2020), https://cprc.org.au/cprc-2020-data-and-technology-consumer-survey/.

Control is particularly lacking given that personal data can often be traded between firms deeply embedded in supply chains without a direct link to consumers or even the basic service they'd signed up for. In addition, it can be difficult for consumers to know where and how to remove their associated data from brokers' holdings.[10] This issue is compounded by terms and conditions and privacy policies that are often ineffective at enabling consumers to make informed choices.[11]

- **Data breaches:** CPRC's consumer research confirmed that while majority of Australians agree that businesses should be responsible for keeping their data safe (84%), there is little to no confidence in businesses actually doing this (less than 26%).[12] In the space of data broking where more means more, data hoarding can lead to numerous sensitive pieces of individual consumer information being exposed to the potential of identity theft and fraudulent activities.

  Example: In 2017, data broker, Equifax, experienced a data breach where hackers gained access to personal information of over 147 million Americans. The data included names, social security numbers, birth dates and addresses.[13] In Australia, Equifax has been found to have issues with data quality, misleading consumers and inappropriate disclosures.[14] The US Consumer Financial Protection Bureau has also reported of data broker insights facilitating scams and fraud.[15]

Combining essential services and data broking – exacerbating the harm

The abovementioned harms are further intensified for those who have no choice with service providers they interact with and the data sharing arrangements those providers may have in place due to their use of third-party applications and tools. The Victorian Office of the Commissioner for Residential Tenancies shared rental insights with CPRC highlighting the increase of data harms for groups such as renters. Renters do not have the luxury to choose the process or the platform that a rental provider or agent utilises as part of the application process.

Renters are also required to disclose significantly more personal information to their landlord or agent compared to many other consumer transactions. This can include photo and other forms of identification, information about their employment and financial history and status. Renters have no control over how this sensitive information is captured, stored or on-sold, other than reliance on the general information privacy principles.

Renters are not the direct consumer of real estate (property management) services. The direct consumer in this case is the property owner. Some protections that apply to consumers of services would not ordinarily apply to groups affected by the delivery of those services like renters. In Victoria, the professional conduct regulations for estate agents have some specific requirements relating to renters. However, these requirements are limited in scope and do not extend to how a potential tenant's data is collected, shared and used by third-party platforms that involve data broking arrangements.

[10] Federal Trade Commission, Data Brokers, "A Call for Transparency and Accountability" (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
[11] Brigid Richmond, "A day in the life of data", (2019), https://cprc.org.au/research-report-a-day-in-the-life-of-data/.
[12] CPRC, "Not a fair trade", (March 2023), https://cprc.org.au/not-a-fair-trade/.
[13] Alfred Ng, "How the Equifax hack happened, and what still needs to be done", (September 2018), CNET, https://www.cnet.com/news/privacy/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/.
[14] Andy Kollmorgen, "Equifax data breach a 'one-off', agency claims", (18 August 2021), CHOICE, https://www.choice.com.au/consumers-and-data/protecting-your-data/data-privacy-and-safety/articles/equifax-security-breach.
[15] CFPB, "Remarks of CFPB Director Rohit Chopra at White House Roundtable on Protecting Americans from Harmful Data Broker Practices", (15 August 2023), https://www.consumerfinance.gov/about-us/newsroom/remarks-of-cfpb-director-rohit-chopra-at-white-house-roundtable-on-protecting-americans-from-harmful-data-broker-practices/.

Question 19: What processes and controls do data brokers have in place to protect consumers? This may include efforts around the de-identification and aggregation of data, data verification processes to ensure data is accurate, or measures to protect stored data. Are these controls adequate? What more could/should be done?

Privacy policies often claim that data sets collected and stored by 'trusted partners' are de-identified, anonymised or aggregated. These 'trusted partners' are often data brokers engaged by the company. However, these practices are inadequate in mitigating consumer harm. De-identified data may not necessarily impact an individual, but its aggregation and use may impact a group or community.[16] De-identified data can also can still be rich and valuable with the potential to be used against others that might fit a similar description but aren't part of the original data set.[17] Furthermore, CPRC research has previously noted that de-identified data such as telephone metadata, transactional history and social network connections can all be re-identified.[18]

The Federal Government must prioritise the following economy-wide reforms to adequately protect consumers from data-based harms:

- Introduce an unfair trading prohibition to protect consumers from businesses that unfairly exploit their customers.
- Reform the Privacy Act to bring Australia's protection framework into the digital age.
- Implement a best-interests duty or duty of care obligations for data-based practices.

Introducing an unfair trading prohibition

Unlike other countries that have prohibitions on unfair practices, business practices that lead to unfair consumer outcomes are currently not illegal in Australia. Examples include business models that:

- predicate on opaque business processes that undermine consumer autonomy
- thrive on profiting from exploiting consumer vulnerabilities, and
- fail to provide accessible and meaningful support to their customers.[19]

Often these unfair business practices target those consumers specifically experiencing vulnerability or disadvantage.[20] Many of the above business models exist within the data broking landscape.

CPRC recommends that the Federal Government prioritise its work on introducing a prohibition on unfair business practices that protects Australians today and in the future. In the context of data broking, it can lead to businesses (first-party data holders and third-party data brokers) considering data-based practices through a lens of fair outcomes for consumers and enable regulators to hold businesses accountable when they fail to do so.

CPRC has conducted a comparative analysis of laws that ban or restrict unfair practices across Europe, the United States, the United Kingdom and Singapore. We have outlined key lessons that Australia can learn from these jurisdictions when implementing its own unfair trading prohibition.[21]

Based on what works well in these jurisdictions, we believe an unfair trading law in Australia should:

[16] Katharine Kemp, "Concealed data practices and competition law: why privacy matters", (5 November 2020), European Competition Journal, Volume 16, 2020 – Issue 2-3, https://doi.org/10.1080/17441056.2020.1839228.
[17] CPRC, "In whose interest: Why businesses need to keep consumers safe and treat their data with care", (March 2023), https://cprc.org.au/in-whose-interest/.
[18] Brigid Richmond., "A day in the life of data", (2019), https://cprc.org.au/research-report-a-day-in-the-life-of-data/.
[19] CPRC, "Unfair Trading Practices in Digital Markets: Evidence and Regulatory Gaps", (March 2021), https://cprc.org.au/unfair-trading-practices-in-digital-market-evidence-and-regulatory-gaps-2/.
[20] CPRC, "Imagining an unfair trading prohibition – CPRC Spark Series Webinar", (September 2022), https://cprc.org.au/event/utpwebinar/.
[21] CPRC, "How Australia can stop unfair business practices", (September 2022), https://cprc.org.au/stopping-unfair-practices.

- be drafted as a principles-based law but with specific guidance or an evolving a blacklist of unfair practices to give clarity to both regulators and businesses
- allow regulators to investigate and proactively enforce the law before widespread harm takes place
- have provisions in place for the law to evolve over time to address new and emerging unfair practices
- hold businesses accountable through penalties and enforcement action that effectively deter unfair business practices
- offer meaningful redress to consumers impacted by unfair practices
- quickly stop practices found to be unfair overseas from making their way to Australia, and
- expand the scope of consumer harm to include the impact on mental health in addition to financial and reputational loss.

Reforming the Privacy Act for the digital age

Our privacy law still relies on notification and consent as the primary means of protecting consumers. By forcing consumers into a situation where they 'decide once' about whether to share their data but bear the consequences potentially for the remainder of their life is not a fair trade.

This reliance on notification and consent means that businesses are practically able to collect significant amounts of data about their customers and use it in almost any way for any outcome. There is currently no protection against businesses embedding consent for personal information to be collected, shared and used (including aggregation with other data points) into long, complex terms and conditions.

At minimum, any reform to the Privacy Act should prioritise protections that go beyond notifying consumers how data will be used or seeking individual consent. Protections should require businesses to stop using data in ways that are highly likely to cause harm.

The Federal Government must fast-track the revision of the Privacy Act 1988 and heed the concerns and proposals made by consumer representatives during the March 2023 consultation on how Australia's privacy protections could be strengthened. Specifically, CPRC urges the Federal Government to:

- modernise what it means to be identifiable to cover information obtained from any source and by any means
- implement genuine privacy by default measures instead of placing the onus on consumers to opt-out of settings that are not designed with their interests in mind
- require all businesses to assess and ensure how they collect and use data leads to fair and safe outcomes that are in the interests of their customers and the community
- empower the regulator to swiftly ban or restrict harmful practices that cause direct and clear consumer harms, and
- provide a clear pathway for redress when things go wrong.

Implementing a best-interests duty or duty of care obligations for data

The interests of Australians must be front of mind for businesses implementing any data-based initiatives. The obligation to act in the interests of others is not new or even unique. For example, the financial sector requires that many professions act in the best interests of customers via fiduciary duties. In sectors such as disability, medical and aged care there is an obligation to act in the interests of others via common law duty of care.

CPRC consumer research confirms that Australians support their data being used with their best interests and the interests of the community in mind. Our national survey found that Australians believe:

- personal information should only be collected and used in a way that personally benefits them (70%)
- their personal information should not be collected and used in a way that harms them or others (83%), and

- personal information should only be collected or used if it is in a person's best interest and is unlikely to cause harm to them and others (70%).[22]

CPRC recommends that the Federal Government embed a best-interests or duty of care obligation as part of its approach to privacy protections which would apply to data brokers as well. Such an obligation would naturally shift the onus of responsibility from consumers to businesses. A best-interests or duty of care obligation would:

- help move away from individual level of consent and shift the focus to system set-up and embedding safety by design
- protect people that may have the inability to consent such as children, people living with a disability or other consumers who are unable to participate in the consent model regardless of how well it may be set-up
- align interests of organisations and consumers as taking on new data will mean taking on new responsibilities and this can encourage a culture of data minimisation (collect only what you need not what you think you might need), and
- address issues of trust and confidence in both government and industry.[23]

A practical option is to consider a best-interests obligation that is broad but is supported by clear guidance and rules, including no-go zones which could evolve over time, with the regulator having the power to regularly review and update guidance and no-go zones instead of them being enshrined in legislation.[24] A similar example of this is the United Kingdom's Financial Conduct Authority's Consumer Duty which has a broad principle to act to deliver good outcomes but is supported with detailed guidance on what that looks like.[25]

Transparency on the involvement of data brokers

You cannot challenge what you don't know. At a minimum, in the interim, while economy-wide reforms are being implemented, the Federal Government should consider labelling requirements for products and services where data captured or used involves the use of data brokers. This transparency will provide a pre-condition for good consumer protection in future, helping regulators, researchers and the general public understand the prevalence of data broking, an awareness that is currently close to non-existent. To ensure labelling is meaningful, the Federal Government should conduct rigorous consumer experience testing prior to developing specific requirements.

Other transparency measures that the Federal Government could also consider include the implementation of a data broker registry, similar to the one that came into effect in 2023 under the New York Privacy Act (NYPA), which also requires data brokers to provide information on how they are meeting consumer rights obligations.[26] However, it should be noted that transparency isn't the only form of consumer protection within New York's Privacy Act that applies to data brokers. It is complemented by the NYPA Data Fiduciary Obligation which requires all businesses to collect, store and use personal information in the best-interest of the consumer.[27] As mentioned previously, making this an enforceable requirement would help shift the responsibility on to businesses to implement practices and business models that aim to deliver fair and safe data-based outcomes for consumers and that aim to mitigate harm.

[22] CPRC, "Not a fair trade", (March 2023), https://cprc.org.au/not-a-fair-trade/.
[23] CPRC, "In whose interest: Why businesses need to keep consumers safe and treat their data with care", (March 2023), www.cprc.org.au/inwhoseinterest.
[24] CPRC, "In whose interest: Why businesses need to keep consumers safe and treat their data with care", (March 2023), www.cprc.org.au/inwhoseinterest.
[25] Financial Conduct Authority (UK), "Finalised Guidance - FG22/5 Final non-Handbook Guidance for firms on the Consumer Duty", (July 2022), https://www.fca.org.uk/publication/finalised-guidance/fg22-5.pdf.
[26] DataGuidance, "New York: Bill for New York privacy act introduced to State Senate", (January 2023), https://www.dataguidance.com/news/new-york-bill-new-york-privacy-act-introduced-state.
[27] Romano Law, "Ready or Not New York, Privacy Here We Come: The Impending New York Privacy Act", (April 2021), https://www.romanolaw.com/2021/04/30/ready-or-not-new-york-privacy-here-we-come-the-impending-new-york-privacy-act.

Question 20: To what extent are consumers aware that their data is being collected and used by data brokers? How are they made aware?

CPRC research confirms that most consumers are unaware of the extent to which they are being tracked.[28] Right now, consumer data can be used by businesses for nearly any purpose. Once consumers have given consent for businesses, usually through vague and lengthy click-wrap consent processes, businesses have little to no accountability for what they do with this data.

To add to the opacity of data brokers, consumers' relationship is often with first-party data sources (the business from which the consumer is using the product or service). As per data broker economy modelling developed by Associate Professor Ramon Lobato, third-party data brokers do not and in fact cannot operate in isolation (see Attachment 1). The data broker business model is intertwined with first-party data sources which provide the catalysts for the data broker model to thrive.[29] Most consumers are unlikely to recognise many of the data broker business names but would be able to easily recall businesses that are first-party data sources. Data brokers are often listed as 'trusted partners' or are noted by name within the fine print of a first-party data source's privacy policy. CPRC's 2020 Data and Technology Consumer Survey confirmed that privacy policies continue to be ineffective in engaging Australians, as 94% of consumers report not reading such information all the time and 33% of consumers never read these documents at all.

It is this intersection between first-party data sources and third-party data brokers that highlights the need for obligations to be placed on all parties, not just a subset within the data space.

Question 21: What steps can consumers currently take to inspect and/or remove the data that is held about them or to otherwise raise a complaint with data brokers?

There is currently limited avenues and no clear pathways for consumers to inspect or raise concerns with data brokers. Under the current Privacy Act, the Australian Privacy Principle (APP) 12 requires organisations to provide individual with access to their personal information upon request and APP 13 provides consumers the right to request correction of personal information. However, the onus is very much on the consumer to know which businesses including data brokers have their data, what data they may have and what other entities have accessed the data through data-sharing arrangements between businesses. The opacity of how businesses engage with data brokers and the limitation of the scope of personal information within the Privacy Act means that the consumer is unlikely to pursue and/or successfully inspect data or request for rectification.

CPRC's 2023 consumer privacy survey confirmed that pursuing recourse action in the data space is a challenging experience. When it comes to redress, 50% of consumers are not aware where to seek redress if they have an issue with how a company collects and processes their data. Similarly, 52% of consumers feel that it is time consuming to find actions to protect their privacy online.[30] This clearly points to the confusion that consumers face in seeking recourse and why it is unlikely that many will not pursue it in the first place.

To better understand the prevalence of requests and complaints made to data brokers, the ACCC could consider using its information gathering powers to:

- understand the quantity and type of consumer data requests that are being made to data brokers and first party sources, and
- what processes are implemented by these businesses to resolve such requests.

[28] Brigid Richmond., "A day in the life of data", (2019), pp. 25-33, https://cprc.org.au/research-report-a-day-in-the-life-of-data/.
[29] Ramon Lobato, "The data broker economy", ADM+S Centre, August 2023, https://www.admscentre.org.au/the-data-broker-economy/.
[30] CPRC, "Not a fair trade", (March 2023), https://cprc.org.au/not-a-fair-trade/.

Question 22: What bodies or resources exist to assist and support consumers in their dealings with data brokers? What more could be done to better educate and empower consumers?

Australians don't currently have a clear and accessible pathway to redress and support when it comes to many facets of the digital economy, including data-based harms. There is no easy, independent way of resolving disputes in the online space.

When consumers are unable to resolve issues directly with a utility like an energy provider or a telecommunications company, they have access to independent support for redress through an ombudsman. However, in the case of redress relating to digital services and technologies, this support is out of reach. Consumers are frequently left to navigate any form of recourse themselves or simply give-up.[31]

CPRC's 2023 consumer privacy survey confirms that Australians are confused about who can help them or where they can get redress if an issue arises with how their data is utilised. They also have high expectations from government to support them on these issues:

- 46% of Australians do not know who to seek help from if they believe their personal information is being used in a way that's causing them harm.
- Only 18% are confident that they will be compensated if they've been left worse-off because of how a company collected, shared or used their information.
- 88% expect governments to protect them against data misuse.
- 85% expect governments to ensure consumers are not opted-in by default to data collection and sharing options. [32]

The Federal Government should finalise and release a scoping study as a matter of priority to identify the types of online disputes consumers are raising along with options for establishing more effective external dispute resolution pathways. CPRC has raised this issue over several Government consultations as we believe there may be merit in a more holistic approach to dispute resolution, such as via the establishment of a Digital Ombudsman that can provide support on all facets of a digital experience.

[31] CPRC, "Australian consumer in their own words", (June 2022), https://cprc.org.au/australian-consumers-in-their-own-words/.
[32] CPRC, "Not a fair trade – Consumer views on how businesses use their data", (March 2023), https://cprc.org.au/not-a-fair-trade.

Attachment 1: ADM+S Data Broker Economy infographic