CHOICE

SUBMISSION TO THE AUSTRALIAN COMPETITION & CONSUMER COMMISSION

DIGITAL PLATFORM SERVICES INQUIRY – MARCH 2024 REPORT ON DATA BROKERS

ISSUES PAPER

AUGUST 2023

57 Carrington Road Marrickville NSW 2204

Phone 02 9577 3333 | Email campaigns@choice.com.au | www.choice.com.au

About Us

CHOICE is the leading consumer advocacy group in Australia. CHOICE is independent, not-for-profit and member-funded. Our mission is simple: we work for fair, just and safe markets that meet the needs of Australian consumers. We do that through our independent testing, advocacy and journalism.

Data brokers pose significant and growing risks to the wellbeing of consumers.

The data broking industry has rapidly expanded in the past decade, which has been assisted by advancements in data science and artificial intelligence. People are increasingly spending more time online, and their personal data is being monetised by an opaque and murky industry.[1] Weak and outdated protections for consumers have allowed data brokers to collect excessive data and expand their reach and power. Although the operation of privacy laws are outside the scope of the Australian Competition and Consumer Commission's (**ACCC**) Inquiry, the intersection of privacy issues with consumer and competition issues warrants discussion in this submission.

There is strong community concern about the use of data brokers. CHOICE research conducted in 2023 found that 76% of Australians were concerned about businesses selling their data to data brokers.[2] People should not be forced to hand over their sensitive personal information to data brokers to simply access essential goods and services.

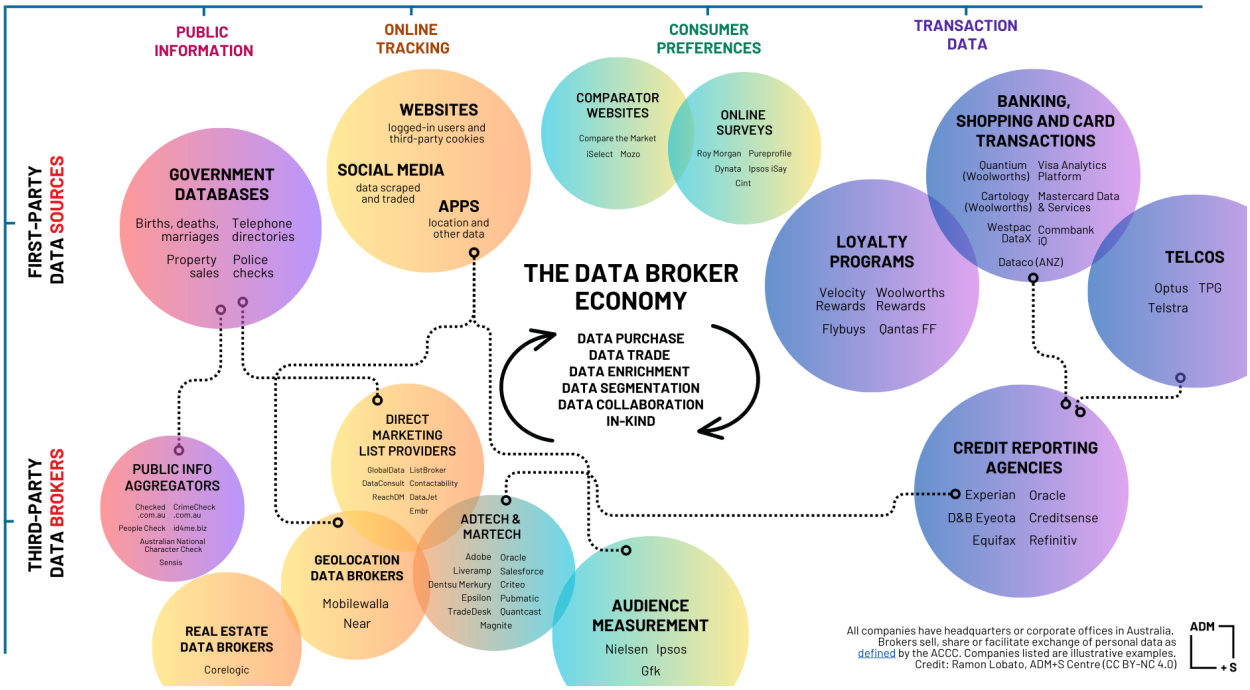
We welcome the ACCC investigating this important issue. This phase of the Digital Platform Services Inquiry comes at a critical time. While data brokers have recently come under increased scrutiny, they still operate in the shadows of our community.[3] This chart, produced by the ARC Centre of Excellence for Automated Decision-Making and Society, uncovers the vast network of data brokers in Australia:[4]

[1] CPRC, 2021, A Day in the Life of Data, https://cprc.org.au/wp-content/uploads/2021/12/CPRC-Research-Report_A-Day-in-the-Life-of-Data_final-full-report.pdf; The Quantum Record, 2023, "How Data Brokers Profit from the Data We Create", https://thequantumrecord.com/blog/data-brokers-profit-from-our-data; FTC, 2014, *Data Brokers: A Call for Transparency and Accountability,* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf; I'MTech, 2019, "Data brokers: the middlemen running the markets", https://imtech.imt.fr/en/2019/11/19/data-brokers-the-middlemen-running-the-markets/

[2] CHOICE Consumer Pulse June 2023 is based on a survey of 1,087 Australian households Quotas were applied for representations in each age group as well as genders and location to ensure coverage in each state and territory across metropolitan and regional areas Fieldwork was conducted from 7th to 22nd of June 27, 2023

[3] WIRED, 2021, "Data Brokers Are a Threat to Democracy", https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy; Politico, 2022, "Data brokers raise privacy concerns — but get millions from the federal government", https://www.politico.com/news/2022/12/21/data-brokers-privacy-federal-government-00072600; Scientific American, 2023, "Science Shouldn't Give Data Brokers Cover for Stealing Your Privacy", https://www.scientificamerican.com/article/science-shouldnt-give-data-brokers-cover-for-stealing-your-privacy

[4] Ramon Lobato, ADM+S Centre, 2023, "The data broker economy", https://www.admscentre.org.au/the-data-broker-economy.



The ACCC has an opportunity to shine a light on this opaque industry. Consumers are best protected when businesses operate in a transparent, safe, and fair market. Without strong laws and regulatory oversight, consumers will continue to experience harms from data brokers.

CHOICE is calling on policymakers to introduce stronger rules on data brokers to ensure people in Australia are protected. This submission also urges the ACCC to expand the scope of its inquiry by including first-party data brokers and credit reporting agencies to better understand the data broking industry.

The ACCC should:

1. recommend the Federal Government implement the recommendations of the Privacy Act Review and increase funding to the OAIC;
2. investigate the role of the Australian Consumer Law in protecting consumers from privacy violations committed by data brokers;
3. recommend the Federal Government to implement a prohibition on unfair trading in the Australian Consumer Law;

4. recommend the Federal Government establish a digital ombudsman; and
5. broaden the scope of the Inquiry to consider first-party data brokers and credit reporting agencies.

Consumers experience a range of harms from data brokers

Data brokers can contribute to a range of harms to consumers. These harms arise from both the data practices of brokers and from the products and services they sell to other businesses. These consumer harms can be categorised into six themes:

1. **Manipulative and discriminatory practices.** Data brokers and their clients can use consumer data to market or provide products that are tailored to consumer characteristics. Research by the Foundation for Alcohol Research & Education has found that vulnerable consumers can be targeted with unhealthy or harmful products based on their personal characteristics.[5] Financial services have also used algorithms to advertise predatory loans and insurance products to people experiencing vulnerability and people of colour.[6] These practices can be facilitated by the use of analytics by data brokers.

2. **Harassment, fraud and scams.** There have been examples of perpetrators using data broking websites to locate and target victims, specifically using people search sites or public information aggregators.[7] These services are also used by criminals seeking information on individuals to facilitate identity theft or scams.[8]

3. **Invasions of privacy by businesses.** Personal and sensitive information which relates to consumers can be collected or inferred by data brokers, despite limitations on this collection by the *Privacy Act 1988 (Cth)* (‘**Privacy Act**’).[9] Consumers face significant financial harm and emotional distress when suffering a

[5] FARE, 2023, *Experiences with online marketing of alcohol, gambling and unhealthy food: A survey,* https://fare org au/experiences-with-online-marketing-of-alcohol-gambling-and-unhealthy-food-a-survey
[6] SBS News, 2018, “The brave new world of ‘surveillance capitalism’”, https://www sbs com au/news/the-feed/article/the-brave-new-world-of-surveillance-capitalism/vfo47kbab; ProPublica, 2018, “Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates”, https://www propublica org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates
[7] The Verge, 2021, “Senators ask FTC to fight stalkers exploiting people search sites”, https://www theverge com/2021/3/4/22313613/ftc-senator-letter-stalking-abuse-data-broker-people-search-sites; Vice News, 2019, “T-Mobile ‘Put My Life in Danger’ Says Woman Stalked With Black Market Location Data”, https://www vice com/en/article/8xwngb/t-mobile-put-my-life-in-danger-says-victim-of-black-market-location-data
[8] Lawfare, 2022, “Data Brokers, Elder Fraud, and Justice Department Investigations”, https://www lawfaremedia org/article/data-brokers-elder-fraud-and-justice-department-investigations
[9] CHOICE, 2022, “Op-ed: Why we need to enforce existing laws against ‘data enrichment’”, https://www choice com au/consumers-and-data/protecting-your-data/data-laws-and-regulation/articles/why-we-need-to-enforce-laws-against-data-enrichment

data breach, including the cost of new identity documents, loss of trust with businesses, and being victims of harassment and fraud.[10] The significant harm of data breaches would be lessened by reducing the scale of data collected and stored by businesses, including data brokers.

4. **Misinformation about individuals.** Businesses can collect inaccurate data about people. Misinformation about consumers can have a range of negative effects, such as damage to their reputation, inability to access financial products such as loans or other forms of credit, or government enforcement agencies receiving false information.[11]

5. **Unfair exchange between consumers and businesses.** Consumers are increasingly expected to provide personal information to access products and services in offline and online settings. This data is financially valuable to businesses, yet consumers may feel they are not receiving a fair exchange for it.[12] Consumers should not be forced to hand over their data to data brokers to access essential goods and services.

6. **Monopolisation of data and anti-competitive behaviour.** As data becomes more valuable, businesses with access to consumer data have grown in market power, which has stifled competition. This is most visible amongst big tech platforms such as Google, Facebook and Amazon which leverage the amount and type of data they collect into market power.[13] There is also a risk that data-sharing practices can create de facto mergers between businesses or cartels.[14]

[10] CHOICE, 2023, "What happens to stolen data on the dark web?", https://www choice com au/consumers-and-data/protecting-your-data/data-privacy-and-safety/articles/stolen-data-on-the-dark-web; ABC News, 2023, "Optus data breach class action launched for millions of Australians caught up in cyber attack", https://www abc net au/news/2023-04-21/optus-hack-class-action-customer-privacy-breach-data-leaked/102247638

[11] WIRED, 2023, "How the US Can Stop Data Brokers' Worst Practices—Right Now", https://www wired com/story/fcra-letter-data-brokers-privacy-regulation; Alexander Tsesis, 2014, "The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data", https://lawecommons luc edu/cgi/viewcontent cgi?referer=&httpsredir=1&article=1502&context=facpubs

[12] CPRC, 2021, *A Day in the Life of Data*, https://cprc org au/wp-content/uploads/2021/12/CPRC-Research-Report_A-Day-in-the-Life-of-Data_final-full-report pdf

[13] Harvard Business Review, 2018, "Here Are All the Reasons It's a Bad Idea to Let a Few Tech Companies Monopolize Our Data", https://hbr org/2018/03/here-are-all-the-reasons-its-a-bad-idea-to-let-a-few-tech-companies-monopolize-our-data

[14] Björn Lundqvist, 2022, "An access and transfer right to data—from a competition law perspective", https://academic oup com/antitrust/article/11/Supplement_1/i57/6696741; Data europa eu, 2022, *Sharing Data (Anti-)Competitively,* https://data europa eu/sites/default/files/report/Sharing_data_anti_competitively_will_European_data_holders_need_to_change_their_ways_under_the_proposed_new_data_legislation pdf; FTC, 2019, "Big Data and Competition Policy: A US FTC Perspective", https://www ftc gov/system/files/documents/public_statements/1543858/big_data_and_competition_policy_china_presentation_2019 pdf

These are only a few significant examples of consumer harms caused by data brokers. Any benefits of data brokers are more likely experienced by businesses they work with rather than consumers, whose data is exploited and monetised.

Data brokers need greater transparency and accountability

The data broking industry owes its success to opaque and unaccountable practices. Consumers have little capacity to access their data from data brokers, which is a laborious and frustrating process.[15] Data brokers often gain access to consumer data through clauses buried in privacy policies that allow for the sharing and trading of data between parties. Privacy policies are notoriously difficult to read and are unread by most consumers. A 2021 CHOICE nationally representative survey found that only 9% of consumers who joined a loyalty scheme always read the privacy policy, while almost a quarter have never read one.[16] Further, privacy policies at best alert consumers to the harms they will face, rather than restrict harmful practices in the first place.

Consumers are dissatisfied with their data being used for purposes other than what people would reasonably expect. CHOICE's nationally representative survey in 2023 found that 65% of consumers were concerned about businesses collecting data about them. 56% of consumers did not trust that businesses were collecting data responsibly and in their best interests.[17] Consumers are also dissatisfied with the way their data is being used. 56% were concerned about how their data was used to personalise products marketed to them, while 76% were concerned about businesses selling their data to data brokers.[18]

Consumers should not be forced to navigate and resolve the complexities of data broking while data brokers are not yet required to mitigate the harms they cause. The most effective mechanism to create transparency and accountability is for the Federal Government to establish strict guardrails on the practices of data brokers. The Federal Government should concurrently establish a digital ombudsman to assist consumers with their rights to redress and accountability.

[15] ABC News, 2018, "I asked everyone from Facebook to data brokers to Stan for my information It got messy", https://www abc net au/news/science/2018-04-28/i-asked-everyone-for-data-from-facebook-to-data-brokers-to-stan/9676700
[16] CHOICE, 2021, "What are loyalty schemes like Flybuys and Everyday Rewards doing with your data?", https://www choice com au/consumers-and-data/data-collection-and-use/who-has-your-data/articles/loyalty-program-data-collection
[17] CHOICE Consumer Pulse June 2023
[18] CHOICE Consumer Pulse June 2023

Data brokers should face stronger regulations

Data brokers are subject to inadequate regulations and oversight. Data brokers should not be trusted to regulate themselves due to a history of harmful and opaque practices.[19]

Many of the steps taken by data brokers to protect personal information are insufficient. As noted by the Issues Paper, data brokers may de-identify and aggregate data to protect consumers. However, studies have demonstrated that this process is often reversible, allowing personal information to be retrieved.[20] Additionally, a limited definition of personal information in the Privacy Act still allows extensive collection of information that can individuate consumers through targeted advertising algorithms and inferred information.[21]

Data breaches highlight the risks of data brokers and other types of mass data collection. In Australia, the scale of the Latitude Financial data breach was partly due to a series of business transitions and mergers that carried consumer data from Coles to GE Money and into Latitude.[22] Abroad, data brokers themselves have been subject to data breaches, including credit agency Equifax which affected around 150 million customers.[23] The financial and emotional cost of data breaches is often irreversible, particularly when it affects survivors of abuse and violence.[24] The scale and impact of data breaches would not be possible without the amount of information collected by businesses such as data brokers, and without the length of time this information is stored.

Data brokers are currently subject to the Privacy Act, but the current regime has proven inadequate in regulating data brokers. This is due to both a lack of enforcement and gaps in the legislation. For example, Dr Katherine Kemp noted that Australian Privacy Principle 3.6 prohibits companies from collecting third-party data to profile consumers,

[19] WIRED, 2021, "Data Brokers Are a Threat to Democracy", https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy
[20] University of Melbourne, 2017, "Research reveals de-identified patient data can be re-identified", https://www.unimelb.edu.au/newsroom/news/2017/december/research-reveals-de-identified-patient-data-can-be-re-identified; The Register, 2021, "De-identify, re-identify: Anonymised data's dirty little secret", https://www.theregister.com/2021/09/16/anonymising_data_feature
[21] Salinger Privacy, 2023, "To fix the Privacy Act, we need one extra sentence", https://www.salingerprivacy.com.au/2023/04/19/one-extra-sentence; Office of the Victorian Information Commissioner, 2018, "The Limitations of De-Identification – Protecting Unit-Record Level Personal Information", https://ovic.vic.gov.au/privacy/resources-for-organisations/the-limitations-of-de-identification-protecting-unit-record-level-personal-information
[22] The Guardian, 2023, "Coles confirms its customers impacted by Latitude Financial data breach", https://www.theguardian.com/australia-news/2023/apr/15/coles-confirms-its-customers-impacted-by-latitude-financial-data-breach
[23] CHOICE, 2021, "Equifax data breach a 'one-off', agency claims", https://www.choice.com.au/consumers-and-data/protecting-your-data/data-privacy-and-safety/articles/equifax-security-breach
[24] ABC News, 2022, "Medibank customers left to endure anxiety and fear without 'right support' after data breach", https://www.abc.net.au/news/2022-11-19/medibank-customers-speak-of-data-breach-impact/101668160

but despite being a common practice for data brokers, this Australian Privacy Principle has not been enforced.[25]

The Attorney-General's Department's Privacy Act Review has documented various gaps in Australia's privacy regime which should be resolved to adequately regulate data brokers. A broader definition of personal information which includes information that "relates to" an individual will ensure the privacy framework is relevant in today's digital environment. A fair and reasonable use test would require businesses to only collect and use data for the purpose of providing consumers with a good or service, and remove unneeded data in a timely manner. Stricter requirements on businesses to gain opt-in consent before direct marketing, targeting, or trading with consumer data would also limit the amount of information data brokers can freely collect.

The ACCC should also consider how privacy and consumer issues intersect in the practices of data brokers, and how the Australian Consumer Law could be an additional mechanism to regulate the practices of this industry. The Federal Government legislating a prohibition on unfair trading would address certain practices that are arguably exploitative or contrary to consumer expectations of fairness in the market. This prohibition could restrict the ability of data brokers and other businesses to collect data through deceptive or manipulative practices, such as dark patterns, subscription traps, and bundled consent.

The ACCC should broaden its report on data brokers

CHOICE urges the ACCC to expand the scope of this Inquiry. The Inquiry should consider including first-party data brokers in their final report, as well as credit reporting agencies. First-party data brokers are defined by the ACCC as "businesses that collect data on their own consumers and sell or share that data with others". Major first-party data brokers include customer loyalty programs and social media platforms.

First-party brokers are capturing an increasing market share of the data broking market. While a number of first-party data brokers were examined in the ACCC's report into customer loyalty programs, it did not cover first-party data analytics businesses that have emerged from other businesses such as Ticketek's analytics subsidiary Ovation or

[25] University of NSW, 2022, "This law makes it illegal for companies to collect third-party data to profile you", https://newsroom unsw edu au/news/business-law/law-makes-it-illegal-companies-collect-third-party-data-profile-you

Afterpay iQ.[26] Without examining first- and third-party data brokers, the inquiry risks forming an incomplete map of the industry.

CHOICE also supports the ACCC investigating data brokers with credit reporting products and services. This would also provide the ACCC with a further understanding of the data supply chain. While many of the functions of credit reporting agencies are regulated separately in the legislation, it is unclear to consumers how major data brokers and credit agencies such as Equifax and Experian separate their operations. This blurry distinction has been criticised internationally and should be considered in an Australian context too.[27] Further, these agencies may have an uncompetitive advantage in their data collection practices due to their existing market share dominance.[28]

Recommendations 1-5

The ACCC should:

1. recommend the Federal Government implement the recommendations of the Privacy Act Review and increase funding to the OAIC;
2. investigate the role of the Australian Consumer Law in protecting consumers from privacy violations committed by data brokers;
3. recommend the Federal Government to implement a prohibition on unfair trading in the Australian Consumer Law;
4. recommend the Federal Government establish a digital ombudsman; and
5. broaden the scope of the Inquiry to consider first-party data brokers and credit reporting agencies.

[26] TEG, 2021, "Cricket Australia & TEG's Ovation in Ground-breaking Data Partnership", https://www teg com au/cricket-australia-tegs-ovation-in-ground-breaking-data-partnership; CHOICE, 2022, "Buy now, pay later providers move into the data business", https://www choice com au/consumers-and-data/data-collection-and-use/who-has-your-data/articles/buy-now-pay-later-data-collection
[27] Duke University, 2022, "Credit Reporting Agencies Don't Just Report Credit Scores", https://techpolicy sanford duke edu/blogroll/credit-reporting-agencies-dont-just-report-credit-scores
[28] Bloomberg Law, 2022, "Startups Take on Equifax, Experian Over Payroll Data Dominance", https://news bloomberglaw com/privacy-and-data-security/startups-take-on-equifax-experian-over-payroll-data-dominance