CHOICE

2 March 2023

Senate Standing Committees on Economics
Via email: economics.sen@aph.gov.au

Inquiry into international digital platforms operated by Big Tech companies

The poor data practices of technology businesses have left people vulnerable to widespread harm. Businesses use automated and data-driven technologies to monitor consumers and invade their privacy, set discriminatory prices, exclude consumers from their services, and buy and sell personal information without the consumer's informed consent.

We have provided the Senate Economics Reference (**the Committee**) with a number of case studies of harm arising from the improper use of consumer's data by major technology companies, including Airbnb and Tinder. However, while not within scope of the inquiry, our investigations have found smaller technology companies and non-technology businesses still contribute significant harm to consumers.

CHOICE will respond to two key topics of the inquiry. First, we will address the harms of automated decision-making (**ADM**) and the need for algorithm transparency and fairness. Second, we will address how consumer data and privacy is exploited and how it can be protected. We recommend a broad range of policy solutions for the Federal Government to protect consumers from these harms.

Algorithm transparency

The rapid growth of algorithms used in ADM by businesses has created a number of risks for consumers. It can create and exacerbate existing discrimination, bias and market inequalities. The use of ADM by businesses can also make inaccurate and wrong decisions. The opacity of algorithms can create barriers to redress for consumers. This also makes it difficult for regulators to identify and address the harms associated with ADM use.

Algorithm transparency will not adequately address the risks associated with ADM by businesses. Policy solutions addressing the harms of ADM must be focused on algorithmic fairness and transparency. Businesses which develop or use algorithms should be required to ensure their algorithms meet community expectations on fairness, safety, and accuracy. Algorithm transparency is also important as it will hold businesses accountable when they fail to act fairly.

CHOICE's investigations into major technology companies Airbnb and Tinder highlight the importance for algorithm transparency and fairness.

Case Study 1 - *Airbnb's social scoring algorithms*

In March 2022, CHOICE investigated Airbnb's algorithm which scores a user's "trustworthiness".[1] The algorithm is able to generate a "social score" of trustworthiness based on personality traits, behaviours, and personal data including social media behaviour. Airbnb can use this score to determine a user's access to their service. Users have no oversight over why and how these decisions are made. Further, the opacity of the algorithm may disguise potentially discriminatory uses of this data, such as inferring a user's sexuality. CHOICE spoke to Airbnb users who were suspended for no reason and without explanation, and other users who were likely suspended for working in sex work.

Case Study 2 - *Tinder's use of algorithmic pricin*g

In August 2020, CHOICE conducted a shadow shop into Tinder's use of algorithmic pricing.[2] Tinder's premium service – Tinder Plus – charges different prices based on a user's age, and may consider other factors such as geographical location or sexuality. For example, a straight male over 50 in a metropolitan area was offered the price of $34.37 for one month. This was almost five times as much as a queer female under 30 in a metropolitan area, who was offered the same service for $6.99. In response to this conduct, Associate Professor Paul Harpur at the University of Queensland said:

> *"There is no reason a person at 25 should be able to access the app cheaper than a person who is 55. This kind of pricing model is discriminatory and would fall foul of Australia's anti-discrimination laws."*[3]

CHOICE wrote a complaint to the Australian Consumer and Competition Commission (**ACCC**) and asked it to investigate whether the conduct of Tinder breached the Australian Consumer Law (**ACL**).[4]

Policy recommendations

We encourage the Committee to consider the following recommendations to improve the regulation of ADM usage by technology and non-technology companies:

[1] CHOICE, Is Airbnb using an algorithm to ban users from the platform?, 21 March 2022, https://www.choice.com.au/airbnb.

[2] CHOICE, Tinder charges older people more, CHOICE, 11 August 2020, https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/tinder-plus-costs-more-if-youre-older.

[3] CHOICE, Tinder charges older people more, 11 August 2020, https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/tinder-plus-costs-more-if-youre-older.

[4] CHOICE, Complaint to the ACCC about Tinder's misuse of data and discriminatory pricing, August 2020, https://www.choice.com.au/consumer-advocacy/policy-submissions/2020/august/complaint-to-the-accc-about-tinder-misuse-of-data-and-discriminatory-pricing.

1. **Legislate a risk-based framework to restrict and prohibit certain uses of ADM.** Consumers do not have strong protections from businesse's use of harmful ADM practices. The Federal Government should legislate a risk-based ADM framework, with restrictions and prohibitions on harmful use. This can be achieved either by:
    a. expanding Office of the Australian Information Commissioner's (**OAIC**) Privacy Impact Assessment compliance scheme to cover private businesses and to incorporate a risk-based framework on ADM; or
    b. establishing separate legislation which regulates the use of artificial intelligence including ADM.

2. **Empower a regulator to protect people from ADM.** The Federal Government should empower an existing regulator with the adequate resources and expertise to regulate ADM. The regulators most suitable for this role would be the ACCC or OAIC. Without strong regulators, consumers may be unfairly discriminated against, excluded, and profiled by ADM systems.

3. **Legislate transparency requirements for the use of algorithms in ADM by businesses.** The use of ADMs is often hidden to consumers. This limits the ability of consumers to provide consent and restricts the ability of regulators and government to assess algorithms. The use of ADM by business should be clearly disclosed on consumer-facing platforms like websites or apps. ADM should also be disclosed in privacy policies in plain language, and should be available for regulators to audit.

Data and privacy

Data breaches can have devastating impacts on Australian consumers, exposing people to financial loss, emotional distress and loss of trust in private markets. In light of recent major data breaches affecting millions of people, the case for strengthening Australia's privacy laws and regulatory enforcement powers has never been clearer.

Businesses profit from monetising consumer data – and not just technology businesses. They often collect unnecessary amounts of data to exploit and on-sell to data brokers. Recent data breaches in Australia were a result of the vast amount of data collected by big and small businesses in recent years, as well as outdated regulations governing data collection.

CHOICE's investigations into loyalty programs and facial recognition technology (**FRT**) highlight the importance for stronger rules regulating consumer data collected by major technology companies and traditional businesses alike.

Case 3 - *Loyalty programs and data monetisation*

CHOICE's research in December 2021 revealed that loyalty schemes are profiting off people's data.[5] Loyalty programs give consumers rewards to encourage repeat business. However, retailers also benefit by obtaining direct contact details of their customers and information such as shopping behaviour for both personalised and aggregate analytics. Consumers in loyalty programs face risks to their data and privacy. This data is regularly shared with partner businesses and data brokers. Data brokers augment data provided by consumers with other sources, such as browsing activity, public records, and financial records. These practices may put consumers at risk of price discrimination and inappropriate profiling by ADM use by businesses.

Case 4 - *The growing use of facial recognition technology (FRT)*

CHOICE's investigation in 2022 found the use of FRT by major Australian businesses in retail settings.[6] Data collection by businesses has advanced to capturing biometric data, including facial features ('faceprints') through FRT. CHOICE found that FRT was used by traditional brick-and-mortar retailers Kmart, Bunnings, and The Good Guys until a pause following CHOICE's investigation and ongoing OAIC investigations.[7] The use of FRT has a number of risks, including data breaches involving biometric data, inaccurate assessments leading to exclusions, and could also hardcode biases such as racial discrimination. CHOICE is concerned that FRT could also be used to further enrich and monetise personal data. Our investigation found that disclosure of the use of FRT is often inconspicuous and without informed consent by consumers.

Policy recommendations

Australia's privacy laws are outdated and are not fit-for-purpose to protect consumers for modern and future uses of information either by major technology companies or non-technology businesses that use digital technology. The Federal Government has released its Privacy Act Review Report and are currently consulting on proposed policy recommendations.[8] We encourage the Committee to consider the following policy recommendations to improve protections for consumers:

1. **Require businesses to have a duty of care over personal data:** A new duty of care provision in the *Privacy Act 1988 (Cth)* (**Privacy Act**) will shift how businesses collect and use consumer data. Currently, many data holders engage in risky data practices, which

[5] CHOICE, What are loyalty schemes like Flybuys and Everyday Rewards doing with your data?, 20 December 2021, https://www.choice.com.au/consumers-and-data/data-collection-and-use/who-has-your-data/articles/loyalty-program-data-collection.
[6] CHOICE, Kmart, Bunnings and The Good Guys using facial recognition technology in stores, 12 July 2022, https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/kmart-bunnings-and-the-good-guys-using-facial-recognition-technology-in-store.
[7] CHOICE, Kmart and Bunnings back down on facial recognition after CHOICE investigation, 28 July 2022, https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/facial-recognition-win.
[8] Attorney-General's Department, Privacy Act Review Report, 2023, https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report.

opens consumers to scams, identity theft, surveillance and exploitative advertising. A legislated duty of care would require entities to take reasonable care not to cause foreseeable harm to consumers through the collection, handling, and use of their data.

2. **Align definitions of "personal information" to consumer expectations.** The current definition of personal information in the Privacy Act is restricted to information *about* a person.[9] However, information *related* to a person and their online activity can be similarly exposed and misused. The current definition should be amended to information that *relates to a person*. An expanded definition would include both inferred data, which is new data generated through personal information, like consumer profiles and behaviour, and technical data, such location data, IP addresses, and device IDs. Businesses can still target individual consumers based on inferred and technical data, and de-identified data can often still be re-identified. An expanded definition will prevent businesses from engaging in data practices which can harm people.

3. **Strengthen the Office of the Australian Information Commissioner.** OAIC is under-resourced and lacks many of the regulatory powers of its consumer protection counterparts, including the ACCC and the Australian Securities and Investment Commission (**ASIC**). A permanent increase in funding will provide OAIC the resources needed to investigate other breaches. It will also allow OAIC to take preventative measures to mitigate the risk of future data breaches.

People need to be protected from unfair trading practices

Consumers still lack legal protections from unfair trade practices. CHOICE supports a new economy-wide prohibition in the Australian Consumer Law which prohibits unfair trading practices. This gap allows businesses to operate unfair business models with limited legal consequences. The ACCC's Digital Platforms Inquiry identified this as an important policy solution which will address consumer harm on digital platforms.[10] Unfair trading laws operate effectively in the United States, European Union, United Kingdom and Singapore.

CHOICE welcomed the commitment in September 2022 by Commonwealth, State, and Territory consumer affairs ministers to consult on proposed reforms to address unfair trade practices. CHOICE strongly recommends the passage of legislation to establish an economy-wide ban on unfair trading.

[9] Privacy Act 1988 (Cth), s 6(1).
[10] Digital platform services inquiry: Interim report No. 5 – Regulatory reform, *ACCC,* September 2022.

Yours sincerely,

Rafi Alam
Senior Campaigns and Policy Adviser
CHOICE