
8 March 2023

Submission to the Senate Economics References Committee: Inquiry into international digital platforms

Submitted via email: economics.sen@aph.gov.au

The Federal Government must fast-track reforms for consumers in the digital economy to ensure Australians are protected from current and future harms.

Australians are currently navigating a digital economy which has not been designed with their best interests in mind. Australians have lost money, lost control over their personal information, or have had their wellbeing impacted by being manipulated into choices that aren't in their interests. Failure to strengthen consumer protections will mean Australians will continue to navigate a digital economy that:

- collects, shares, and uses data to make predictions about consumers in ways that can leave them worse-off
- uses and aggregates data to unfairly exclude consumers from accessing certain products and services
- targets consumers to expose their vulnerabilities for commercially beneficial outcomes
- fosters little transparency on what consumers are presented, what they consume and at what price, and
- lacks adequate support for consumers seeking redress from data-related harms.

The answer, however, is not a one-size-fits-all solution. The Federal Government must prioritise the following economy-wide reforms to deliver a holistic consumer protection framework that effectively holds digital platforms accountable across all their business sectors:

- Introduction of an unfair trading prohibition to protect consumers from businesses that unfairly exploit their customers.
- Reform of the Privacy Act to bring Australia's protection framework into the digital age.
- Introduction of a general safety provision to clearly make companies responsible for delivering safe, secure data-driven products and services.
- Increased enforcement resources for regulators to proactively operate within a complex digital environment.
- Clear pathways for consumers to access support when experiencing digital harms.

CPRC is a not-for-profit consumer policy think tank. 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.

Our submission uses insights from our 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 Committee 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.

Yours sincerely



Chandni Gupta
Digital Policy Director
Consumer Policy Research Centre

Market concentration

Question 1: What impact does the market power of big tech companies have on the economy, society and small businesses?

While large digital platforms promise the abundance of choice in products and services, they continue to leverage their market power in a way that benefits them but often leaves consumers worse-off.¹ Previous CPRC research² has revealed numerous examples of practices from digital platform services³ that can lead to consumer harm, many of which are unfair but currently not illegal in Australia. These practices, summarised below, represent externalities that have a negative effect on consumers.

Below are harms that consumers typically experience from digital platforms:

- **Manipulation:** sophisticated companies can have the power to design online user interfaces in very manipulative ways, for example, by using dark patterns.⁴ Companies can use the information they hold 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.⁵ 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.⁶
- **Discrimination and exclusion:** information about consumers can be and is used to benefit commercial entities in discriminatory ways at direct odds with the needs and interests of consumers.⁷ 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).⁸ 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.⁹ Profiles can also be used to set prices, leading to some groups of consumers paying more for the same service.¹⁰
- **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.¹¹ 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

¹ CPRC, “The Digital Checkout”, (December 2021), <https://cprc.org.au/the-digital-checkout/>.

² See: Brigid Richmond, *A Day in the life of data*, 2019, CPRC, pp. 34-40. CPRC also funded a research project that provided a literature review on data tracking. See: University of Melbourne, *State of the Art in Data Tracking Technology*, 2019

³ The *Issues Paper* (p. 13) sets out the “data services providers” who design services for analysing and/or have access to information about consumers, including Data Management Platforms, Data Analytics Services and Data Brokers.

⁴ “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).

⁵ 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>.

⁶ CPRC, “Duped by design - Manipulative online design: Dark patterns in Australia”, (June 2022), <https://cprc.org.au/dupedbydesign/>.

⁷ University of Melbourne, *State of the Art in Data Tracking Technology*, 2019, p. 14.

⁸ Wolfie Christl, “Corporate Surveillance in Everyday Life”, (June 2017), Cracked Labs, p. 13, https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf.

⁹ Cathy O'Neil, “Weapons of Math Destruction”, (2016), Crown Books, p. 143.

¹⁰ For an example of personalised pricing, see 2020 investigation by Choice where it found that people over the age of 30 were offered prices more than double the prices of those aged under 30: <https://www.choice.com.au/about-us/media-releases/2020/august/tinders-secret-pricing-practices>.

¹¹ CPRC, “CPRC 2020 Data and Technology Consumer Survey”, (December 2020), <https://cprc.org.au/cprc-2020-data-and-technology-consumer-survey/>.

how to remove their associated data from brokers' holdings.¹² This issue is compounded by terms and conditions and privacy policies that are often ineffective at enabling consumers to make informed choices.¹³

Due to the opacity of digital supply chains, consumers may have little to no direct relations with specific actors within the digital platform services where these risks stem from.

Question 2: What regulatory measures could be put in place to address the adverse impact of big tech companies? What other non-regulatory interventions could governments take to reduce the market power of big tech companies?

Question 3: Do Big Tech companies have any special dispensations from the rules that govern all other companies? If so, should these be removed, and why?

Australians are currently navigating a digital economy which has not been designed with their best interests in mind. The existing regulatory framework in its current form is not fit-for-purpose – it was not designed with digital platforms being part of the supply chain. As an example, currently there is a lack of clarity on how the Australian Consumer Law (ACL) applies to digital platforms, given that the law was established well-before the introduction of large digital platforms.

In the case of supply of goods or services, the term supply in the Competition and Consumer Act (CCA) is narrowly defined as, "...in relation to goods—supply (including resupply) by way of sale, exchange, lease, hire or hire-purchase".¹⁴ As digital platforms often consider themselves as a 'facilitator of the supply' but not the actual supplier, it creates loopholes in accountability which would be difficult to close via traditional compliance and enforcement measures. This is particularly the case where digital platforms operate an online retail marketplace, creating a scenario where consumers are often left with the burden to resolve issues with the third-party seller on their own. This is further exacerbated when the third-party seller is based overseas – in these cases an Australian consumer technically has rights under the ACL but enforcing them is likely impossible.¹⁵

CPRC recommends that a review of Australia's current competition and consumer protection frameworks needs to be undertaken without further delay to address these types of gaps. Key issues that need to be urgently addressed include:

- updating merger and acquisition frameworks by taking into account the factors that contribute to Big Tech companies (and potentially other business models in future) becoming dominant in the market (such as the acquisition of existing or potential competitors, the economies of scope gained from additional data sets and growing network effects)
- restricting the ability of Big Tech companies to treat the products and services they offer more favourably than other similar products offered by third parties, such as by introducing specific rules banning self-preferencing, or forcing platforms to separate functions, and
- introducing bespoke competition regimes for digital platforms that have strategic market status within the economy (similar to legislation that has been introduced in Europe via the Digital Markets Act).^{16 17}

¹² 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>.

¹³ 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/>.

¹⁴ See: *Competition and Consumer Act 2010*, Retrieved from <https://www.legislation.gov.au/Details/C2011C00003>.

¹⁵ CPRC, "The Digital Checkout", (December 2021), <https://cprc.org.au/the-digital-checkout/>.

¹⁶ CPRC, "The Digital Checkout", (December 2021), <https://cprc.org.au/the-digital-checkout/>.

¹⁷ See Digital Markets Act (DMA) came into force on 1 November 2022 and will take effect from 2 May 2023: https://competition-policy.ec.europa.eu/dma_en.

Algorithmic transparency

CPRC urges the Federal Government to consider specific safeguards in ensuring fairness and safety of consumers in the context of artificial intelligence. Algorithmic bias which can be inherently present in AI-powered decision-making tools can lead to unfair treatment and discrimination.¹⁸ Transparency alone cannot be the only measure of compliance for businesses.

Emerging technologies featuring algorithmic decision-making have the potential of becoming embedded across all facets of a person's life over the coming years. CPRC research has found that 79% of consumers think government has a high level of responsibility to ensure personal information is not used to make consumers worse off.¹⁹ Given this, it will be critical that a genuine effort is made to ensure Australians can clearly see, understand and trust how artificial intelligence (AI) and automated decision-making (ADM) systems are being used and what the benefits are to them.

Failure to get the settings right will lead to direct harm and a loss of consumer trust. As noted by the Australian Human Rights Commissioner, "...*algorithmic bias can cause real harm. It can lead to a person being unfairly treated, or even suffering unlawful discrimination, on the basis of characteristics such as their race, age, sex or disability.*"²⁰

CPRC's research in partnership with the Australian Human Rights Commission notes that transparency is only one facet of promoting responsible business use of AI and data. In addition, the following principles are critical to include in AI and ADM architectures to ensure the focus is on delivering improved consumer outcomes:

- **Accessibility:** Markets are inclusive, and all consumers have the right to access this technology and its application on an equal basis with others.
- **Accountability:** Consumers have a clear route for seeking explanations and accessing appropriate redress from a responsible party if things go wrong.
- **Agency:** Consumers are empowered to exercise autonomy and freedom of choice in their interactions with technologies such as AI systems and the use of their personal data.
- **Transparency:** People are made aware when they are the subject of a decision-making process that uses an AI system.
- **Understandability and explainability:** Individuals subject to these decisions are entitled to a meaningful, comprehensible explanation of the AI system and its decision-making process.
- **Sustainability:** Long-term implications of technology on consumers are considered and addressed throughout design and implementation.²¹

We recommend that the Government also prioritise the development of innovation enablers to support technology that will create genuine benefits for all Australians. Innovation enablers should include:

- investing in and enabling AI and ADM innovation in the not-for-profit sector to demonstrably improve community outcomes and welfare, and
- implementing regulatory sandboxes to enable the safe testing and learning environment prior to deploying AI and ADM-enabled products and services at scale.

¹⁸ Australian Human Rights Commission, "Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias" (2020), <https://tech.humanrights.gov.au/downloads>.

¹⁹ CPRC, "CPRC 2020 Data and Technology Consumer Survey", (December 2020), [CPRC 2020 Data and Technology Consumer Survey - CPRC](#) – CPRC, page 30

²⁰ AHRC, "Using artificial intelligence to make decisions", (November 2020), [Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias \(2020\) | Australian Human Rights Commission](#)

²¹ *Ibid.*

Data and privacy

Question 1: What benefits would arise from introducing a legal mechanism to allow people to seek compensation for privacy breaches in Australia (e.g. establishment of a statutory tort for serious invasion of privacy)?

Australians don't currently have a clear and accessible pathway to redress when it comes to many facets of the digital economy. 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 telecommunications company, they have access to independent support for redress through an ombudsman. However, in the case of redress relating to an online experience, this support is out of reach. Consumers are frequently left to navigate any form of recourse themselves or simply give-up.²² For some complaints, consumers may be able to raise issues through state-level tribunals, but these processes tend to be difficult to navigate and take long periods.

Several participants in CPRC's qualitative research conducted in 2021, specifically noted not pursuing redress options for products or services purchased online, as they felt the likelihood of being compensated was low. In absence of support, consumers are left powerless, with no pathway to compensation.

CPRC strongly recommends that the Federal Government 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. This work should consider digital issues today and complex matters that are likely to arise in the future. CPRC has raised this issue over a number of 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.

There must be effective dispute resolution pathways to enable consumers to seek redress for when things go wrong in the online space. As consumers increase their engagement online, a Digital Ombudsman needs to be adequately resourced to meet benchmarks for industry-based customer dispute resolution to ensure consumers can effectively resolve any disagreements that will arise.²³

Question 2: Would stronger penalties levied by government regulation act as an effective disincentive to prevent data leaks and hacks in the future? What should be the scope and size of any such penalties?

Stronger penalties can be an effective disincentive to prevent data leaks and hacks but only if they are backed with effective enforcement. Businesses must be held accountable and penalties need to be commensurate with the harm caused to consumers via poor business practices.

For legislation and its respective penalties to be effective, they need to be supported by regular surveillance and enforcement by the regulator to educate and shift the market towards a more consumer-centric approach to the digital economy.

Australia needs well-resourced regulators with the capacity and capability to monitor and enforce breaches in the complex digital environment. Traditional compliance and enforcement models often take place post harm. This needs to be reimaged if protection is to be adequately delivered to consumers in the digital economy.

²² *Ibid.*

²³ See: [Benchmarks for Industry-based Customer Dispute Resolution | Treasury.gov.au](#)

Regulators also need more sophisticated approaches to identify harm. Currently regulators largely rely on reports from consumers, identifying harm after it takes place. The majority of the onus cannot continue to remain on consumers to identify and report breaches. This is not feasible in a digital environment where there is little to no transparency about how consumer data is collected, used, and passed on to other businesses. Instead, regulators need to proactively uncover harm that is currently obfuscated. Regulators should be pushing businesses to be radically more transparent about how they use consumer data – this is a first step to then removing unfair practices.

Monitoring and surveillance by regulators in this complex environment needs a diverse workforce that not only understands the implications of the law but also the technical architecture on which these business models are built upon. Experts such as data scientists, artificial intelligence engineers, information security analysts and other technical professionals need to be in the mix to support upstream regulation and mitigate the risk to consumers, potentially before widespread harm has occurred.

Question 3: Do further changes to privacy laws in Australia need to be made to better protect Australians and change corporate attitudes regarding data collection and management?

Australia's privacy protections are currently stuck in the 1980s, pre-dating not only the digital economy but internet itself. Australians deserve better. Australia's 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 starkly contrasts with the knowledge and capability of firms to understand the value and potential use of data.

Any reform to the Privacy Act should prioritise protections that go beyond notifying consumers how data will be used or seeking individual consent. It should require businesses to stop using data in ways that are highly likely to cause harm. The reform should ensure that Australia has a well-resourced regulator that can undertake strong proactive enforcement and has adequate redress measures for Australians when they've been harmed by poor privacy protections.

However, reforming the Privacy Act is only part of the solution. CPRC recommends the adoption of a broader framework to ensure potential harms across the digital economy can be adequately addressed. A broader framework should require online businesses to show evidence of how they mitigate and/or reduce the risk of harms to consumers. The approach should place the onus back on businesses instead of where it is currently – with consumers via reporting mechanisms and regulators via investigations of identified breaches.

In addition to reforming the Privacy Act, wider whole-of-economy reforms are needed to adequately protect consumers, such as:

- introducing an unfair trading prohibition – expanded on further below
- introducing a general safety provision, and
- introducing an obligation for businesses to use data in consumers' best-interests – expanded on further below.

Australia needs to stop unfair business practices

Unlike other countries that have prohibitions on unfair practices, several business practices that lead to unfair consumer outcomes are currently not illegal in Australia. Examples include business models that thrive on high-pressure sales of low value products, that fail to provide accessible and meaningful support to their customers and are predicated on opaque business processes that

undermine consumer autonomy. Often these unfair business practices target those consumers specifically experiencing vulnerability or disadvantage.²⁴

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. CPRC has conducted a comparative analysis of laws that ban or restrict unfair practices across Europe, the United States, the United Kingdom and Singapore and has outlined key lessons that Australia can learn when implementing its own unfair trading prohibition.²⁵

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

- 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
- expand the scope of consumer harm to include the impact on mental health in addition to financial and reputational loss.

Incorporating a best interests duty or a duty of care

Introducing economy-wide measures also brings the opportunity to incorporate elements that may not have yet been considered in competition and consumer protection frameworks for digital settings. Incorporating a duty of care or best-interests duty (similar to a fiduciary duty), especially for how consumer data is treated and how choice architecture is presented and implemented on digital platforms, can help add a level of accountability on digital platforms that could significantly reduce the likelihood of consumer harm. It could also lead to pro-business benefits by increasing consumer trust in those platforms that actively build this into their business model.

The idea of a best interests duty for consumer data is relatively new and unexplored in the Australian context. As a next step, CPRC recommends an inquiry to explore how to construct and implement positive obligations on businesses to use data in consumers' interests.

²⁴ CPRC, "Imagining an unfair trading prohibition – CPRC Spark Series Webinar", (September 2022), <https://cprc.org.au/event/utpwebinar/>.

²⁵ CPRC, "How Australia can stop unfair business practices", (September 2022), <https://cprc.org.au/stopping-unfair-practices>.

The Metaverse

Question 1: Given the currently ambiguous status of the Metaverse and its development, is it necessary to begin regulating it now, or should authorities wait in order to understand better how it will function?

We are beyond the waiting game now when it comes to developing adequate consumer protections for products and services in the digital economy. It is clearly evident that a self-regulatory or self-assessed approach is no longer adequate in addressing the risks posed to consumers by large and powerful digital platforms. We need the Federal Government to be proactive and not wait for Australians to endure harm first before creating safeguards for them.

Australians expect and deserve legislation that holds businesses accountable for their practices. We need to evolve our laws to broader principles that capture unfair practices and require businesses like digital platforms to think broadly about how they help rather than hurt consumers.

Implement a principles-based approach to safe use of technology and data

CPRC recommends that the Federal Government consider a more principles-based approach to rule-making that is technology neutral and can capture digital products and services that are available today and in the future. In the first instance, we recommend the Federal Government to review and consider international models for data and digital innovation that are people-centric and aim to actively mitigate harm. One such example is that of New Zealand. In 2018, the New Zealand Privacy Commissioner released principles for safe and effective use of data, which could be considered in the Australian context:

- **Deliver clear public benefit** – use of data must have clear benefits for all citizens.
- **Ensure data is fit for purpose** – use the right data, in the right context and be aware of how data is collected and analysed (including accuracy, precision, consistency and completeness of data).
- **Focus on people** – consider how the use might impact on people such as their privacy and protection against misuse of information.
- **Maintain transparency** – ensure citizens know what data is held about them, how it's kept securely, who has access to it and how it's used (including a well-documented process of data use and analysis).
- **Understand the limitations** - ensure decision-makers are informed of the limitations of analytical processes and the data to predict and describe outcomes (check for biases and other harmful elements).
- **Retain human oversight** – human oversight for decision-making should never be entirely replaced. Decisions based on automated processes affecting people should be disclosed and reviewed to preserve fundamental rights and freedoms.²⁶

Insights from CPRC's digital research program highlight what Australian consumers expect the laws governing the collection, sharing and use of their data to deliver:

- **Fairness** – entities do not collect, share and use data in a way which is unfair, exploitative or extractive.
- **Safety and security** – entities are obligated to keep consumers safe.
- **Choice and control** – consumers are provided with genuine, meaningful control and choice over their data.
- **Transparency** – entities are required to be transparent about why, what and how data is being collected, shared and used with consumers and citizens.

²⁶ Privacy Commissioner (New Zealand), "Principles for safe and effective use of data analytics", (2018),

<https://www.privacy.org.nz/publications/guidance-resources/principles-for-the-safe-and-effective-use-of-data-and-analytics-guidance/>

- **Accountability** – entities and individuals are held to account for data misuse, enforcement is effective, and remedies are easily obtained.
- **Inclusion** – consumers are not excluded nor receive detrimental outcomes as a result of data collection, sharing and use by entities.

These principles can be applied to any form of digital innovation. To ensure these principles are enshrined in how markets operate within our digital economy, the Federal Government should aim to embed the principles through reforming the Privacy Act and by introducing a prohibition on unfair trading practices. These principles should also be front of mind for Government when developing future regulation that impacts data and digital practices.

Big Tech disinformation

Question 2: Should the Australian Code of Practice for Disinformation and Misinformation, which is currently voluntary, be enshrined into the law (as has been done in the EU)?

CPRC recommends that the Australian Code of Practice for Disinformation and Misinformation should be enshrined into law. Digital platforms should be obligated to report their compliance with the code to a regulator that is adequately resourced to assess and enforce the code. Compliance reporting must be transparent so businesses can be publicly accountable for their performance against the obligations.

Digital platforms and their business models are no longer developing or new. Initiatives such as voluntary codes of practice that are self-assessed are no longer adequate in addressing the risks posed to consumers by large and powerful digital platforms.

Consumers expect and deserve legislation that holds businesses accountable for their practices. We need to evolve our laws beyond voluntary commitments to broader principles that capture unfair practices and require businesses like digital platforms to think broadly about how they help rather than hurt consumers.

The time to act is now

CPRC urges the Federal Government to implement the range of measures outlined in this submission without further delay to ensure the digital economy delivers equitable outcomes to all Australians. Many of the measures, such as restricting unfair business practices and establishing strong privacy protections have been in place in other jurisdictions for decades. Failure to protect consumers will mean that Australians will continue to be exposed to business models that manipulate consumer consent, use opaque business processes that undermine consumer autonomy or exploit consumer vulnerabilities. Australian consumers deserve better.