Consumer Policy Research Centre

Level 6, 179 Queen Street, Melbourne, Victoria 3000

ABN 23 100 188 752 T 03 9639 7600 W cprc.org.au

Submission to the Productivity Commission on 5-year Productivity Inquiry: Australia's data and digital dividend

20 October 2022

Submission made via: https://www.pc.gov.au/inquiries/current/productivity/interim2-data-digital

Dear Commissioners

Innovation in data and digital services is not an end in itself. Innovation must be guided to deliver positive outcomes for all Australians. How data is collected, shared, used and aggregated needs adequate guardrails so data-led innovations do not lead to Australians being worse-off.

The Consumer Policy Research Centre (CPRC) welcomes the opportunity to provide a submission to the Productivity Commission's Inquiry into Australia's data and digital dividend.

CPRC urges Government to adopt a people-centric mindset when considering innovation in the digital economy.

The Federal Government needs to implement a range of measures to protect consumers and ensure that the data and digital dividend delivers equitable outcomes. We recommend that the Government:

- implement a principles-based approach to guide the safe use of technology and data
- resolve major policy issues required to develop an enabling environment by reforming the Privacy Act and introducing stronger consumer protections
- embed the practice of conducting a cost-benefit analysis as part of data and digital framework that identifies direct benefits to Australians
- enshrine a 'duty of care' on business use of consumer data.

Failure to protect Australians will mean people 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 people from accessing certain products and services
- targets people to expose their vulnerabilities for commercially beneficial outcomes
- fosters little transparency on what people are presented, what they consume and at what price
- lacks adequate support for people seeking redress from data-related 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 inquiry using three key principles – fairness, safety and inclusivity for consumers engaging in the digital economy.

We would welcome the opportunity to work with the Productivity Commission and share further insights from our consumer research projects. For further discussion regarding our research and the contents of this submission, please contact

Yours sincerely

Chandni Gupta
Digital Policy Director
Consumer Policy Research Centre

Recommendation direction and information request 3.5: Supporting ethical use of technology and data

- How should government support the ethical adoption of new uses of technology and data, particularly for applications outside of artificial intelligence?
- What would be the benefits and costs of any government activity on technology and data ethics?
- If some regulation is required in Australia on ethical issues, how can the government identify high-risk settings where regulation would be most appropriately targeted?

CPRC believes there is greater value in implementing clear guardrails to digital and data innovation instead of focussing on more esoteric references to ethics. There needs to be clear guardrails that ensure that adoption and development of new technology does not cause harm to Australians. Having clear rules for innovation and use of data will create the trust required for consumers to engage in the digital world in a way that fuels further, positive innovation. Without clear and clearly enforced protections, we can expect that people will rightly lose trust, opt-out or actively stop using digital tools.

The various data and digital reform processes currently underway across the Australian Government need to be guided by clearly articulated principles. Without it, the Government is at great risk of developing a policy environment which is not joined up or coherent. In turn, this will result in conflicting approaches, processes, standards and outcomes, which will reduce productivity as well as undermine investment and community trust. Consumers also expect this reform: when it comes to unfair and harmful data practices, our research shows that 94% of Australian consumers expect government to protect them against the collection and sharing of their personal information.[1]

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

CPRC recommends that the Government 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.[2]

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.

[1] CPRC, "CPRC 2020 Data and Technology Consumer Survey", (December 2020), https://cprc.org.au/cprc-2020-data-and-technology-consumer-survey/.
[2] 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/

- **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.
- **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.

To ensure these principles are enshrined in how markets operate within our digital economy, the Australian Government should aim to embed the principles via the Australian Data Strategy, 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.

Resolve major policy issues required to develop an enabling environment

CPRC recommends that the Government prioritise the following reforms to protect consumer data and build trust in further data and technology advances:

- Reform the Privacy Act to bring Australia's protection framework into the digital age.
- Introduce an unfair trading prohibition to protect consumers from unfair data extraction and digital misuse.
- Introduce a general safety provision to clearly make companies responsible for delivering safe, secure data-driven products and services.
- Establish rules or protocols to ensure that deidentified consumer data cannot be re-identified.[3]
- Introduce impact assessments for government reforms to data and technology, which include a cost-benefit analysis to truly identify the value of new digital innovations and to whom will it benefit the most – consumers, or entities with a commercial interest.
- Increase enforcement resources for regulators within a complex digital environment.
- Establish clear pathways for consumers to access support and redress when experiencing digital harms.

These reforms should result in businesses using consumer data to boost consumer benefits rather than cause harm. It should lead to consumers having genuine and meaningful control over their data with adequate controls and protections.

With the review of the Privacy Act currently underway, we recommend urgent economy-wide reforms to address the increasing ubiquity of data collection, use and disclosure in the economy which in turn, would also help inform the various digital reforms that will sit beside it (e.g. Consumer Data Right regime). Implementing the Privacy Act reforms will ensure the environment surrounding digital innovation in data-enabled products and services provides sufficient protection for consumers, including data that becomes part of Australia's open data sources. Clearer market stewardship is required from governments to ensure that emerging digital markets both work for and deliver benefits for all Australians.

Embed cost-benefit analysis and success metrics as part of data and digital framework that identifies direct benefits to Australians

CPRC strongly recommends that the Government conduct and publish cost-benefit analysis and success metrics for government-led projects and government-initiated investigations that relate to new and emerging technologies and data innovations. This is particularly pertinent for high-risk initiatives that directly impact people's lives. As an example, to date there has not been a cost-benefit analysis of

[3] As an example, the NSW Government specifically notes the use of a Personal Information Factor tool to assess re-identification risk as part of its strategy to publish COVID-19 cases and tests data. See: Case Study: Personal Information Factor (PIF) Tool | Data NSW.

the current implementation approach of the Consumer Data Right nor have consumer-centric success metrics been established, despite these being recommended by various consumer organisations across several consultation processes.[4]

A cost-benefit analysis should be conducted prior to public release to identify the value that the system will bring and to remove or mitigate any consumer harms. As an example, facial recognition has been introduced into the community without due consideration of the risks this technology can pose to society. As such the technology has been implemented by businesses such as Bunnings, Kmart and The Good Guys that are not in the digital innovation space, nor have the capacity to appreciate and mitigate the risks linked to such technology.[5] If a cost-benefit analysis is prioritised early, it would enable Government to place guardrails and implement targeted compliance initiatives, well before the technology is rolled out at mass.

A key element of the cost-benefit analysis should also give due consideration to factors that contribute to vulnerability. Our research on vulnerability notes the importance of integrating vulnerability principles in a work program and developing clear aims, indicators and measures that are specific to consumer vulnerability.[6] This is also a concept that is currently being applied in the UK Office of Gas and Electricity Markets where cost-benefit analysis now includes a specific weighting for vulnerability.[7]

Enshrine a 'duty of care' on business use of consumer data

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. They can use the data to manipulate customers, to steer them towards products or options that are not in the consumers' best interest or even on-sell the data to commercial partners. We need a way to hold businesses more accountable for what they do with data, as well as how it is stored and kept safe.

When considering a governance framework for emerging technologies, the concept of a "duty of care" is a principles-based approach to holding businesses accountable in implementing people-centric outcomes as part of their deployment of new technology and data-driven models. The idea of a duty of care in a digital setting is relatively new and unexplored in the Australian context. Incorporating a fiduciary duty, especially for how consumer data is treated and how it is processed by business models, can help add a level of accountability on entities that could significantly reduce the likelihood of consumer harm. It further shifts the focus towards 'doing right by people'. It could also lead to pro-business benefits by increasing consumer trust in those platforms that actively build this into their business model. As a first step, CPRC recommends that the Government consider a law reform inquiry to explore how to construct and implement positive obligations on businesses to use data and emerging technologies in consumers' interests. This could be explored through a review of the Competition and Consumer Act including the Australian Consumer Law to ensure it is fit-for-purpose for the digital economy.

[4] CPRC, "Submission: Statutory Review of the Consumer Data Right – Issues Paper", (May 2022), https://cprc.org.au/submission-statutory-review-of-the-consumer-data-right-issues-paper/.
[5] CHOICE, "Kmart, Bunnings and The Good Guys using facial recognition technology in stores", (July 2022), https://www.choice.com.au/facialrecognition.
[6] O'Neill, E, "Consumer Data Right Report 1: Stepping towards trust Consumer Experience, Consumer Data Standards, and the Consumer Data Right", Consumer Policy Research Centre, (February 2021), Consumer Data Right Report 1: Stepping towards trust Consumer Experience, Consumer Data Standards, and the Consumer Data Right - CPRC.
[7] Presentation by Meghna Tewari, Head of Retail Market Policy (Ofgem) at the 2021 ACCC/AER Regulatory Conference (Session 2B – Consumer vulnerability and market design).

Recommendation direction and information request 3.6: Coordinating the policy and regulatory environment

- Whether there is evidence that poorly coordinated policy and regulatory activity in digital, data and cyber security areas have negatively affected businesses' investment, innovation or productivity?
- What policy issues and regulations are most important for agencies to coordinate on domestically and/or internationally, including both current and emerging areas?

The focus of policy and regulation of digital innovation cannot continue to remain purely on how it impacts industry alone. Measuring innovation and productivity without considering the impact on consumers paints an incomplete picture. When considering the policy and regulatory environment, Government must take into account consumer outcomes and harms as a result of adopting and deploying new technologies. The previous Government's online compliance intervention system, robodebt, is a classic example of where poorly coordinated policy in fact benefitted government investment, innovation and even productivity at the time, generating $1.7 billion in debts. However, it failed to comprehend the impact of or implement adequate safeguards for rolling out a beta system on the most vulnerable groups of the community.[8] CPRC recommends that the Productivity Commission take a broader view when assessing the impact of policy and regulation and not limit it to effects on industry.

In terms of international collaboration on policy issues and regulations, CPRC recommends that Australian agencies coordinate with their international counterparts especially in relation to current and emerging data and digital regulation. Government must consider what the net effects are in terms of new laws being introduced in other jurisdictions that apply to global businesses that also operate in Australia. For example, the recent introduction of both the Digital Markets Act and the Digital Services Act in Europe, combined with Europe's current directive on unfair commercial practices are likely to have a significant shift in how businesses operate and adjust their business models. It is naïve to assume that a global business will naturally course correct across all jurisdictions. Often this is not the case, especially when they are benefitting from current business models.

As an example, in July this year, Amazon changed its cancellation process for its Prime membership subscription to a simple two-clicks with a clear cancellation button after it was found to have breached EU's unfair trading laws.[9] This change has not been implemented in Australia. Currently, Australians are navigating through multiple screens, multiple steps and multiple options. In this last screen the customer is offered four options, and three of the four involve keeping Prime in some form. Only one is about immediate termination but unlike the EU where the option stands out (Figure 1), here in Australia it blends in with all the others (Figure 2).[10]

[8] Brookes, J., "Robodebt was technology 'beta testing' on most vulnerable citizens", (8 September 2021), https://www.innovationaus.com/robodebt-was-technology-beta-testing-on-most-vulnerable-citizens/.
[9] European Commission, "Consumer protection: Amazon Prime changes its cancellation practices to comply with EU consumer rules", (1 July 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_4186.
[10] CPRC, "How Australia can stop unfair business practices", (September 2022), https://cprc.org.au/stopping-unfair-practices/.

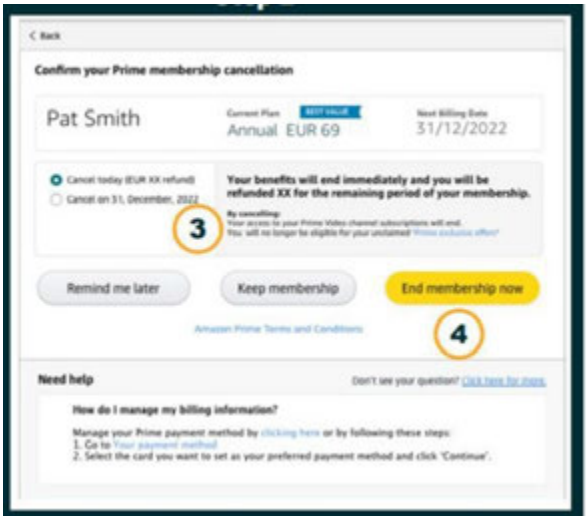

Figure 1: Updated final screen for cancelling Amazon Prime subscription in Europe
Source: European Commission: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_4186

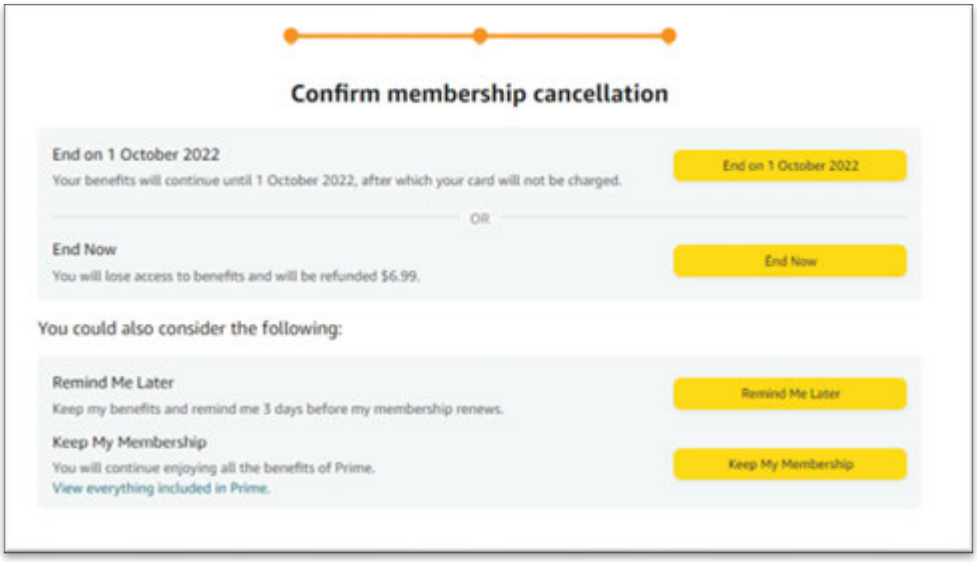

Figure 2: Final screen for cancelling Amazon Prime subscription in Australia where the process involves a range of dark patterns (deceptive designs) that aim to influence and manipulate consumer behaviour.

This type of business practice is known as dark patterns which are design features and functionalities built into the user interface of websites and apps that purely exist to influence consumer behaviour. Dark patterns are extremely prevalent and cause consumer harm. CPRC research found 83% of Australians have experienced negative consequences as a result of dark patterns that are aimed at influencing their behaviour. Australians have lost money, lost control of their data or have been manipulated by a business to make a choice that was not in their interest.[11]

Other jurisdictions appear to be making strides in digital and data innovation but with rigorous safeguards, placing high-level of accountability on businesses. It would be in Australia's best interest to coordinate with international jurisdictions to learn from the measures that have been put in place and collaborate on how digital and data innovation can be embedded into Australia's digital economy with effective protections that mitigate harm for Australians.

[11] CPRC, "Duped by design - Manipulative online design: Dark patterns in Australia", (June 2022), https://cprc.org.au/dupedbydesign/.

Recommendation direction and information request 3.2: Creating new data sharing and integration opportunities

What would be the essential features of a policy requiring healthcare providers to share data on patient services and outcomes with and through government as a condition of receiving government funding, including:

- how to stage implementation in a way that supports providers with different constraints and capabilities, and recognises the potential costs that some stakeholders would face
- what data would be required to be shared, weighing up the likely benefits associated with greater use of specific data items against the costs of providing that data
- how government could work with software providers to co-design and, ultimately, automate reporting requirements
- could My Health Record (MHR) be the starting point for implementing this data sharing requirement and, if so, what changes would be required for this broader use of the MHR system?

Government should thoroughly assess challenges in the current system before implementing obligations for the use of any system and setting implications for not doing so.

Consumers largely want health care providers to have the information they need to provide quality care. According to research conducted by Consumers Health Forum (CHF), Australians are supportive of their health data being shared among their healthcare providers – 80% are ready to share their health data in a digitally enabled health system.[12]

"They want providers to input their health information in a central place and want them to use it as they move across the health system where they encounter multiple health providers. As they see the expansion of digital health their increasing frustration at consistently having to repeat their medical history to numerous providers is obvious." – CHF Submission to the National Interoperability Plan.[13]

Processes must ensure there is seamless flow of health data with relevant health providers. This is critical given that according to Australian case law, a doctor's duty of care does not include providing the patient a copy of the doctor's records.

"*Where that duty can be performed without giving the patient access to the doctor's records, there is no foundation for implying any obligation to give that access."* – High Court of Australia decision on ownership of medical records.[14]

CPRC supports CHF's recommendation made across other consultations and papers for the need of conducting a clear assessment of barriers, one of which seems to be low interoperability of current health software with the My Health Record. Government must ensure barriers are addressed first before linking use with receipt of government funding.[15] Failing to do so will negatively impact Australian patients more than the medical practitioners. Patients will be the ones who will be required to bear the extra costs that would have otherwise been covered through rebates.

[12] CHF, "The future of healthcare in Australia: designed for consumers, enabled by digital, accessible for all", (2 March 2022), https://chf.org.au/media-releases/future-healthcare-australia-designed-consumers-enabled-digital-accessible-all.
[13] CHF, "Draft National Interoperability Plan", (December 2021), https://chf.org.au/sites/default/files/20211213_draft_national_interoperability_plan_submission.pdf.
[14] High Court of Australia, "Julie Breen v Cholmondeley W Williams (1996) 186 CLR 71", (6 September 1996), Canberra.
[15] CHF, "Draft National Interoperability Plan", (December 2021), https://chf.org.au/sites/default/files/20211213_draft_national_interoperability_plan_submission.pdf.

Recommendation directions and information requests 3.3: Developing digital, data and cyber security skills

How could the skilled migration program be made more relevant to current and future digital and data skill needs — for example, by improving the occupation list or changing how skilled visas are granted?

There is a concerning lack of role diversity involved in regulating businesses that utilise or profit from complex digital and data-driven models.[16] As an example, the opacity of how businesses collect, share and use data and the impact on people are still not well-understood or effectively scrutinised by governments. Regulators should be pushing businesses to be radically more transparent about their business models and practices – this is a first step to then mitigating unfair digital and data practices. However, this is only possible when the traditional enforcement model, currently leaning heavily on legal and economic expertise only, is reimagined as 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.

Professions such as ethical designers, data scientists, artificial intelligence experts and information security analysts can all play a valuable role in an enforcement framework to ensure innovation in the data and digital space is safe and meaningful for Australians. However, none of these professions (with the exception of Information and Communications Technology (ICT) security specialist) are currently on the skilled migration occupation list.[17] CPRC recommends that the Government review the skilled migration occupation list to ensure it is attracting professionals that can contribute to Australia's current and emerging data and digital ecosystems.

[16] CPRC, "Duped by Design – Manipulative online design: Dark patterns in Australia", (June 2022), https://cprc.org.au/dupedbydesign.
[17] Department of Home Affairs, "Skilled occupation list", (Last accessed: 11 October 2022), https://immi.homeaffairs.gov.au/visas/working-in-australia/skill-occupation-list#