

Submission by Consumer Policy Research Centre to Australian Human Rights Commission – Human Rights and Technology Discussion Paper

26 March 2020

By email: tech@humanrights.gov.au

Dear Mr Santow,

The Consumer Policy Research Centre (CPRC) would like to thank you for the opportunity to respond to the AHRC's Human Rights and Technology Discussion Paper.

CPRC is an independent, not-for-profit consumer research organisation. CPRC undertakes interdisciplinary and cross-sectoral research to inform policy reform and practice change. Our goal is to achieve a fair outcome for all consumers. Consumer data is a central research priority for the organisation due to the rapidly growing online marketplace, increasing adoption of digital technology by Australians, and the emerging benefits and risks to consumers of big data amalgamation.

This submission draws from an evidence base of research and policy engagement by the CPRC. Our work in this area includes: two independent consumer data research reports, *Consumer Data and the Digital Economy* (2018) and *A Day in the Life of Data* (2019); experience advising policymakers and regulators through forums including the Open Banking Data Standards Body and the National Data Advisory Council; and ongoing interactions with CPRC's Consumer Data Research Network (with membership spanning disciplinary research areas across AI, machine-learning, privacy, consumer behaviour, competition law, and consumer law). As well, in the past two years we have lodged public submissions to consultations including the ACCC's Digital Platforms Inquiry; the Department of Industry, Innovation and Science's AI Ethics Framework; and a number of responses in relation to the new Consumer Data Right legislation and associated instruments.

In this submission, we first expand on three core recommendations reflecting on the broader policy environment and highlighting some of the central issues in relation to rights and needs of citizens and consumers in a data-driven society:

- *People should have agency over how technology affects their life choices, chances and trajectories;*
- *Government should provide economy-wide protections for consumers and citizens;*
- *Civil society should be equipped for balanced and inclusive policy debate and reform.*

Second, we discuss six principles for data-driven technologies and regulation: transparency; understandability; agency; accessibility; accountability; and sustainability. We suggest these are key principles for an integrated and cross-jurisdictional policy framework that is capable of supporting

effective, rights-based governance in relation to data, AI, and emerging technologies; while also encouraging choice, innovation, and competition for healthy markets and consumer empowerment.

Overall, we emphasise the need for rights and autonomy of individuals to be protected by government through a more cohesive approach to oversight and regulation of AI-informed decision-making technologies, and the control and use of consumer data more generally. We also propose that for this to be achieved it is appropriate and prudent for the Australian Government to increase investment to regulatory bodies tasked with the monitoring and evaluation of digital markets and emerging technologies, and the enforcement of laws and regulations in this area.

Our submission brings a consumer lens to the question of human rights and technology, and does not seek to address all matters raised by the Commission's Discussion Paper. In other respects our response has taken a broader purview, surfacing consumer-relevant issues regarding human rights and technology that enlarge themes beyond the Discussion Paper's focal areas of AI-informed decision-making, and accessibility as it pertains to people with disability. For ease of reference, we have flagged where our comments have affinity with specific proposals set out in the Discussion Paper.

1. General recommendations

1.1 *People should have agency over how technology affects their life choices, chances and trajectories*

The scaling up of computational power and corresponding convergence of physical, digital and biological technologies into connected networks of unprecedented scope, velocity, and systems impact has been described by the World Economic Forum as the Fourth Industrial Revolution¹. This changing landscape of production, management, and governance – and the technological innovations associated with its evolution – have clear potential to create benefits at individual and societal levels, many of which are identified in the Commission's Discussion Paper. As well, if they are not designed inclusively and implemented responsibly, new technologies carry immense potential for social damage and human disadvantage as individuals increasingly lose control over how technology affects their life choices, chances and trajectories.

Arguably one of the biggest threats to human rights in this context, and of specific concern for consumer rights, is widespread opacity surrounding data collection, sharing, and use; and the corresponding erosion of people's agency over choices and opportunities affecting their everyday lives and future prospects. While such issues may not be new in themselves, effects prior to the advent of big data tended to be incremental and localised, whereas impacts are now playing out at exponential scale and across all facets of consumer experience.

By expanding collection and analysis of data and the resulting application of this information, a layer of intelligence or thinking manipulation is added to processes and objects that previously did not have that layer... As information tools and predictive dynamics are more widely

1 <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>

adopted, our lives [are] increasingly affected by their inherent conclusions and the narratives they spawn. The overall impact of ubiquitous algorithms is presently incalculable because the presence of algorithms in everyday processes and transactions is now so great, and is mostly hidden from public view.²

In today's economy, data is a critical input to production: providing raw inputs and deriving refined outputs. Control over this commodity is a highly sought-after source of market power, evidenced by the rise in data brokerage business models and a thriving ad tech industry fuelled by loyalty schemes, tracking cookies, and the widespread digital transformation of social, civic, and purchasing behaviours and interactions. However, the rise in technology companies' capacity to cultivate, harvest, process, and profit from data as a direct or indirect by-product of people's online activity has not been matched by commensurate consumer awareness regarding how their data is being manipulated and on-sold. As the US Federal Trade Commission explained in a report calling for greater transparency in the data trade:

Data brokers acquire a vast array of detailed and specific information about consumers; analyze it to make inferences about consumers, some of which may be considered sensitive; and share the information with clients in a range of industries. All of this activity takes place behind the scenes, without consumers' knowledge³.

Growing information asymmetry between consumers and data holders – characterised by a lack of transparency in online terms of service, privacy policies, and other data-related terms of use – has created an environment where profiling and exploitative practices with regard to the retailing of data and consequent provision and pricing of services are increasingly common. Mutability of terms after acceptance, without informing users of such changes, is also unfair and a common problem identified by consumer advocates and regulators. These and other issues associated with information asymmetries in consumer environments have been recognised by governments in many parts of the world, including Australia, where the recent ACCC Digital Platforms Inquiry produced a number of recommendations aimed at strengthening consumers' privacy rights, transactional bargaining power, and control over their data⁴.

One area of particular concern for protecting consumer rights is the way in which ad tech business models deliberately profile, target, and manipulate consumer vulnerabilities. A study released by Privacy International in 2019 surveyed the data practices of 136 European websites hosting online information or services relating to mental health conditions such as depression and anxiety, and the extent to which they share and on-sell data to third parties without informing users. This research found that over 70% of the surveyed websites included embedded trackers for Google's DoubleClick advertising services, and approximately 40% were sharing data with Facebook. Most sites included multiple third-party trackers performing a common function of using cookies with unique identifiers to

2 Chudakov, B. quoted in Rainie, L. and Anderson, J. (2017) *Code-Dependent: Pros and Cons of the Algorithm Age* <https://www.pewresearch.org/internet/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/>

3 Ramirez et. al. (2014) *Data Brokers: A Call for Transparency and Accountability* US Federal Trade Commission, pvii. <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>

4 Recommendations 16-21; ACCC (2019) *Digital Platforms Inquiry Final Report*, Australian Competition and Consumer Commission <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>

track users across the web (and across different devices) to create granular user profiles, including the fact that people have visited mental health websites. Many of these third-party tracking cookies were placed prior to users being given an option to express – or deny – consent. Some of the websites included trackers from data brokers and ad tech companies known to engage in programmatic advertising, “a practice that is under increasing scrutiny by European regulators and which raises specific privacy concerns when used on health-related websites”:

When data brokers, advertisers and online tracking companies collect data about our mental health without our knowledge or consent, this is highly intrusive. Information that reveals when exactly someone is feeling low or anxious – especially if combined with other data about their interests and habits – can be misused to target people when they are at their most vulnerable⁵.

Data profiling based on consumer health choices may also affect consumer agency in healthcare decisions more directly. For example, fitness and lifestyle tracker data is regularly used as means for ‘incentivising’ health insurance; initiatives by John Hancock Financial⁶ in the USA and Qantas⁷ in Australia being two recent examples where voluntary data provision is overtly framed as being for consumer benefit without flagging the potential for this type of data collection to become a basis for raising premiums or reducing coverage should it reveal high risk lifestyle or health conditions.

Also in the insurance sector, use of predictive genetic information by life insurers has been restricted in several international jurisdictions, and was flagged by the Australian Parliamentary Joint Committee on Corporations and Financial Services 2018 Inquiry into the Life Insurance Industry as an area of concern, with the Committee recommending a moratorium on allowing life insurers to use outcomes of predictive genetic tests⁸. The progress of this pause will be relevant to, for example, consumers who might become aware of (and are currently obliged to disclose) a genetic predisposition through the purchase and use of genealogical DNA tests.

Healthcare markets are also instructive in providing representative examples of how algorithmic data matching and analysis and machine learning techniques can be used to deliver positive benefits targeted to local contexts⁹; and where these practices can have negative impacts on a range of human rights, including the right to health. For example, IBM Watson’s Oncology AI has come under fire for providing faulty or unsafe advice when suggesting treatment options for cancer patients¹⁰; while UnitedHealth’s Impact Pro algorithm was assessed by New York lawmakers as being racially

5 <https://privacyinternational.org/report/3193/report-your-mental-health-sale>

6 <https://www.theverge.com/2018/9/26/17905390/john-hancock-life-insurance-fitness-tracker-wearables-science-health>

7 <https://insurance.qantas.com/termsfuse>

8 Australian Parliamentary Joint Committee on Corporations and Financial Services (2018) *Inquiry into the Life Insurance Industry* https://www.aph.gov.au/-/media/Committees/corporations_cte/LifeInsurance/report.pdf

9 van’t Hoog, A.H., Onozaki, I. & Lonnroth, K. (2014) ‘Choosing algorithms for TB screening: a modelling study to compare yield, predictive value and diagnostic burden’, *BMC Infectious Diseases* 14. <https://doi.org/10.1186/1471-2334-14-532>

10 <https://www.telegraph.co.uk/technology/2018/07/27/ibm-watson-ai-criticised-giving-unsafe-cancer-treatment-advice/>

discriminatory in effect after it was shown to result in poorer treatment outcomes for African American patients than for white patients with comparable health issues¹¹.

While the examples discussed above are all drawn from health markets, the data practices and business models they illustrate are domain agnostic, as are the underlying issues of how consumer control and relevant protection of data rights can have significant and ongoing implications for life choices, chances and trajectories. Data reform must prioritise the rights of individuals to exercise agency with regard to making – and contesting – decisions and actions that affect them, and should continue to evolve mechanisms for consumers (and citizens) to be informed, included, and in control of their data across all sectors. The application of big data, technology and AI should enhance rather than restrict the capacity of persons to participate in society, including access to markets and agency in consumer choice.

Efforts towards achieving this recommendation can be strengthened through the adoption of ‘Rights by Design’ approaches such as those outlined in Proposals 13, 25, 26, and 27 of the Commission’s Discussion Paper. We also support the use of Regulatory Sandboxes as a way of testing and strengthening compliance of AI-informed decision-making systems with human rights (Proposal 15) and other legal obligations. In relation to Question F(b), we suggest regulatory sandboxes might also be usefully applied to test systems compliance with consumer rights legislation, including rules and obligations arising from the new Consumer Data Right.

1.2. Government should provide economy-wide protections for consumers (and citizens)

Consumer knowledge, organisational transparency, and formal review channels are necessary to build trust and maintain capability for the involvement and agency of citizens, and to protect consumer rights to contest actions/decisions in all markets. In some cases relevant protections already exist in the Australian Consumer Law and other legislation, however the cross-sector and transnational reach of new technologies has rendered grey areas that are not sufficiently tested by and/or protected in law. Technology is changing at a rapid rate, making it difficult for regulators and policymakers to make sector-based rules in consumer environments where predicting the next technology advancement is not always possible.

Benefits of an economy-wide approach to privacy and data rights are detailed by the ACCC in the final report of their 2019 Digital Platforms Inquiry. Among these benefits, the ACCC notes that an economy-wide approach to addressing problematic data practices will ensure that consumers transacting in diverse markets receive consistent consumer protections and welfare improvements, including protecting consumers using digital platforms in cases where their personal information is shared with third parties that would not be covered under a digital platform specific regime¹².

CPRC strongly supports establishment of economy-wide protections and principles-based regulation. Such frameworks prioritise the achievement of clear and enforceable regulatory objectives over highly

11 Akhtar, A. (2019) *New York is investigating UnitedHealth’s use of a medical algorithm that steered black patients away from getting higher-quality care* <https://www.businessinsider.com.au/an-algorithm-treatment-to-white-patients-over-sicker-black-ones-2019-10>

12 ACCC (2019) *Digital Platforms Inquiry Final Report*, p452.

prescriptive regulation that is heavily focused on compliance rules. Our view is that prescriptive regulation often comes at the expense of an adaptive framework that “allows for technological advancement without needing regular detailed amendment,” as discussed in Chapter 3 of the Commission’s Discussion Paper. Conversely, legislation that is principles-based and economy-wide enables regulatory frameworks to be flexible enough to respond to emerging opportunities and risks. Section 2 of this submission discusses in more detail a set of six key principles that we suggest are supportive of establishing harmonised protections in law and policy.

Acknowledging the interpretive uncertainty that can arise from principles-based regulation in application, we also emphasise the need for sufficient government investment in a robust regulatory enforcement and co-regulatory support regime. This accords with the position stated by the ACCC in its *Digital Platforms Inquiry Final Report* (2019), which emphasised that the Office of the Australian Information Commissioner (OAIC) must be “adequately resourced to fulfil any new responsibilities stemming from broader reforms to the Australian privacy framework in addition to carrying out its existing functions”¹³. By way of illustration, the ACCC reports that introduction of the GDPR raised standards of protection for EU residents’ personal information and also created increased workload for many data protection authorities, drawing attention to Ireland as one jurisdiction where government funding for regulators was adjusted to meet demand, with the 2019 budget allocation to Ireland’s Data Protection Commission increasing by €3.5 million to €15.2 million¹⁴.

CPRC firmly believes that Australia will benefit from economy-wide consumer protection and privacy reforms of a similar nature to the EU’s General Data Protection Regulation (GDPR), or the California Consumer Privacy Act in the USA. Although some elements of the GDPR have been criticised as imposing an unreasonable compliance burden, many of the core objectives underpinning these regulations – including rights to information, comprehensibility, and accuracy; to data access, erasure and portability; and to be informed of, object to, and contest the results of automated decision-making – are essential for shifting unfair advantage away from powerful conglomerates and data brokers.

We also wish to draw attention to the responsibility of government to consider additional measures that may be necessary to safeguard the data rights of children:

*Too often, children do not know what rights they have over their own data and do not understand the implications of their data use, and how vulnerable it can leave them*¹⁵.

As individuals who are increasingly active in online environments prior to having reached a developmental stage where they might be expected to have a full understanding of consequences associated with their behaviours, children require special protection in law. For example, the UK’s 2018 Data Protection Act makes provision for an age-appropriate design code requiring companies to implement privacy-by-design features in order to obtain parental consent before collecting and

13 ACCC (2019) *Digital Platforms Inquiry Final Report*, p477.

14 Data Protection Commission Ireland Press Release, 9 October 2018, *Data Protection Commission welcomes significant increased funding of €3.5 million in 2019 Budget* <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-welcomes-significant-increased-funding-eu35>

15 Fore, H. UNICEF (2019) An Open Letter to the World’s Children <https://www.unicef.org/child-rights-convention/open-letter-to-worlds-children>

processing data of children under the age of thirteen; and establishes a ‘right to innocence’ enabling people to request social networks delete anything they posted before the age of eighteen.

Today’s children are the first generation growing up at a time of rapid datafication where almost all aspects of their lives, both on and off-line are turned into data points. An entire generation of young people is being datafied – often starting even before birth... The potential uses of such large volumes of data and the impact on children’s lives are unpredictable, and could potentially be used against them¹⁶.

Alongside identified issues with surveillance capitalism in the form of data profiling, Australians have raised concerns over the integration of visual and aural surveillance technologies (incorporating facial and voice recognition) into everyday products, services, and public spaces¹⁷. Such technologies often have a valid functional reason for collecting data in the first instance, however the creation of large composite datasets for machine learning – or other purposes which may be opaque or unspecified – has significant implications for the rights of consumers and citizens.

Much has been written about the potential for personal harassment and professional damage to be perpetrated through deepfakes leveraging voice and image data¹⁸; and the dangers to civil rights contingent on compilation of facial recognition databases¹⁹. Consumer concerns regarding how data they provide intentionally is repurposed and reused, in combination with additional data harvested from their movements in physical and online spaces, are exacerbated by a lack of transparency regarding the intent and extent of how such technologies are being deployed. Recommendations of the Australian Parliamentary Joint Committee on Intelligence and Security’s *Advisory Report on the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019* highlight the critical need for transparency of purpose and use in relation to government implementation of such technologies, as well as the importance of legislation to include mechanisms governing ongoing oversight and reporting²⁰. While government protections regarding its own use of technology are vital, the extension of economy-wide protections has a broader remit.

Extreme power asymmetries between consumers and suppliers in data-driven dealings can create unfairness in consumer markets, a situation which is exacerbated by the absence of an unfair trading prohibition in Australian Consumer Law (ACL). These concerns have been voiced by the ACCC who, in making a formal recommendation for a prohibition against certain unfair trading practices as part of their 2019 Digital Platforms Inquiry, found:

16 Young, A., Campo, S., and Verhulst, S. (2019) *Responsible Data For Children: Synthesis Report* UNICEF/GovLab <https://rd4c.org/images/rd4c-report-final.pdf>

17 See, for example <https://www.zdnet.com/article/australias-surveillance-laws-are-hitting-the-social-license-problem/> and <https://www.smh.com.au/technology/privacy-concerns-mount-as-drones-take-to-the-skies-20151208-glijyk.html>

18 Kietzmann, J., Lee, L.W., McCarthy, I., and Kietzmann, T. (2020) ‘Deepfakes: Trick or treat?’ *Business Horizons*, 63:2, pp.135-146.

19 *Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties*, US House of Representatives Committee on Oversight and Reform; Hearing May 22, 2019. <https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-1-its-impact-on-our-civil-rights-and>

20 [https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024343/toc_pdf/Advisoryreportonthelidentity-matchingServicesBill2019andtheAustralianPassportsAmendment\(Identity-matchingServices\)Bill2019.pdf](https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024343/toc_pdf/Advisoryreportonthelidentity-matchingServicesBill2019andtheAustralianPassportsAmendment(Identity-matchingServices)Bill2019.pdf)

...ubiquity of data collection and use, by both digital platforms and other businesses, and the resulting increased potential for significant harm to consumers, demands consideration of the current protections provided to consumers by the ACL in relation to these practices²¹.

In addition to coverage outlined by the ACCC report, we suggest an unfair trading prohibition in the Australian Consumer Law could also encompass unfair trading practices contingent on AI-informed decision-making and enhanced data profiling, including where:

- businesses use AI-based decision-making to frustrate the exercise of consumer rights and challenges to decision-making about essential and important services (e.g. access to energy, telecommunications, basic banking products and affordable credit)
- businesses are not transparent with consumers about AI-informed decision-making and data profiling and do not obtain meaningful, informed consent to these practices.

Similarly, there is currently no general safety provision in the Australian Consumer Law despite recommendations for such being made by a 2017 review of the ACL and a subsequent motion of the Senate in 2018²². Our view is that a general safety provision in consumer law – including consideration of data manipulation and reuse practices – would help to secure protection and enhance agency of consumers with regard to how their personal data is processed by systems vendors and market service providers.

As well, we strongly support reform of Australia's Privacy Act as a fundamental step towards ensuring that greater transparency is provided for all in the data ecosystem²³. Industry leaders have similarly emphasised the need for action in this area, with Apple Chief Executive Tim Cook publicly advocating in 2019 for more comprehensive legislative approaches to data privacy and regulation:

Right now, all of these secondary markets for your information exist in a shadow economy that's largely unchecked — out of sight of consumers, regulators and lawmakers²⁴.

Lessons from international practice indicate that overarching policy frameworks for data and AI should be coordinated, consistent, and championed. Technology does not exist in a bubble, and government interventions must take into account intersectional and transnational contexts. In 2020, the European Commission published their *White Paper on Artificial Intelligence: a European approach to excellence and trust*²⁵, extending on 2018's *Coordinated Plan on AI* by outlining a policy framework designed to create an 'ecosystem of excellence' along the entire value chain by establishing incentives to accelerate the adoption of AI within a cohesive regulatory framework aimed at creating an 'ecosystem of trust'. Accompanying the white paper release, a *European Strategy for Data* specifically proposes that a cross-sectoral governance framework for data access and use is necessary to create an "over-

21 ACCC (2019) *Digital Platforms Inquiry Final Report*; p498 and Recommendation 21.

22 Australian Senate Hansard, Thursday 23 August 2018, p5681.

23 CPRC (2019) *A Day in the Life of Data*.

24 Cook, T. (2019) *You Deserve Privacy Online. Here's How You Could Actually Get It* <https://time.com/collection/davos-2019/5502591/tim-cook-data-privacy/>

25 European Commission (2020) *White Paper on Artificial Intelligence: a European approach to excellence and trust* https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

arching framework for the data-agile economy, thereby avoiding harmful fragmentation of the internal market through inconsistent actions”²⁶.

Jurisdictions worldwide are already testing how to implement new policy and regulation across overlapping areas of privacy, human rights, competition and consumer protection. General data protections provided for by the EU’s GDPR have been taken up by lawmakers beyond EU borders and are being modified and reflected in laws such as the California Consumer Privacy Act (2018); the UK Data Protection Act (2018); and Thailand’s Personal Data Protection Act (2019), which was drafted based on the GDPR (although with some significant material differences, such as the omission of comparable provisions in relation to automated individual decision making, including profiling)²⁷.

We propose that in order to achieve appropriate protection for citizens, and to remain competitive in global markets and research environments, Australia cannot afford to lag in this regard.

The recommendation for economy-wide protections and corresponding resourcing by government is of particular relevance for Proposals 1, 2, and 19 of the Commission’s Discussion Paper. Respectively, these call for: a *National Strategy on New and Emerging Technologies*; an independent body to enquire into ethical frameworks for new and emerging technologies; and the establishment of an AI Safety Commissioner as a new statutory office. We suggest that each of these measures would be considerably strengthened by ongoing consideration of how they harmonise with economy-wide frameworks and existing initiatives.

1.3 Civil society should be equipped for balanced and inclusive policy debate and reform

CPRC agrees with the Commission’s position that developing and maintaining an effective policy framework for Australia’s AI and data protection regime will require input from many channels. Effective policy reform calls for the informed and active participation of citizens to accurately reflect social values; as well as awareness and training within industry and education sectors to instigate and support inclusive research, design and co-regulatory efforts; and the willingness of government to seek out and respond to diverse views. Without this distributed involvement, projected gains from digital transformation are unlikely to eventuate.

*Part of what we’re gonna have to understand is that if we want the values of a diverse community represented in these breakthrough technologies, then government funding has to be a part of it. And if government is not part of financing it, then all these issues ... about the values embedded in these technologies end up being potentially lost or at least not properly debated*²⁸.

26 European Commission (2020) *Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions: A European strategy for data*, p12. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN>

27 <https://hsfnotes.com/employment/2019/07/31/thailand-personal-data-protection-act-to-take-effect-in-may-2020/>

28 Obama, B. (2016) in *The President in Conversation With MIT’s Joi Ito and WIRED’s Scott Dadich* <https://www.wired.com/2016/10/president-obama-mit-joi-ito-interview/>

We agree that any *National Strategy on New and Emerging Technologies* should seek to secure government resourcing dedicated to education and training for government, industry and civil society (Proposal 1(d) of the Discussion Paper), and that this should incorporate community education on AI and human rights (Proposal 16). We also suggest that these measures should extend to similarly ensure resourcing for initiatives that facilitate direct participation of consumer and citizen stakeholders in sharing their views and input regarding new technologies, including where such technologies relate to data rights and regulation and AI-informed decision-making. We draw attention to the views of global leaders such as then-US-President Barack Obama (quoted above) in highlighting the necessity for government to support this level of participation in order to obtain social license for, and equitable outcomes from, new technologies.

Policy that does not proceed with end-users in mind, or which does not adequately address concerns voiced about new technologies, will not be trusted and is unlikely to produce optimal outcomes. A local example of this is visible in the lower than predicted uptake of the Australian government's My Health Record initiative, a trend reflected across both consumers and providers of health services²⁹. Design flaws in My Health Record that were identified in the lead up to launch of the technology included a failure to take sufficient account of specific concerns around data privacy in family violence contexts, so that an estranged parent would potentially have visibility of the location of children, putting those children (and other family members) at risk of harm. More broadly, as surgeon Neela Janakiraman identified in an analysis of the technology from a medical practitioner's perspective: "we know that as soon as people worry about medical privacy, they simply avoid presenting for care at all"³⁰.

Janakiraman also cautioned that consumers of health services experiencing vulnerability across a range of factors would be disproportionately affected by barriers to understanding the risks and accessing the benefits of My Health Record:

They ... may not have computers. They may not know how to access their MyGov account or navigate to their My Health Record. They may not have the computer or language skills to access or understand their record, even if they can access it at a public library or other location. They may not know how to edit or delete records. They may not understand what their doctor is asking [if] it is suggested that an event summary be uploaded after an appointment, and thus may not be giving truly informed consent as to what is being uploaded about them.

The 'techlash' surrounding implementation of My Health Record presents a textbook example of how opportunities for socially beneficial uses of data and technology are compromised when the predominant perceptions and experiences of consumers are ones of opacity and data misuse.

As elements in building up social trust and wider capabilities for civic and consumer participation in data technology reform, CPRC agrees that the Australian Government should conduct a comprehensive overview of how AI is being used in public sector decision-making, especially where this may involve the combining of private sector and public sector data (Proposal 17), and should

29 Minion, L. (2017) *GPs and hospitals claim My Health Record is not fit for purpose as alarmingly low usage figures are released* <https://www.healthcareit.com.au/article/gps-and-hospitals-claim-my-health-record-not-fit-purpose-alarmingly-low-usage-figures-are>

30 <https://womensagenda.com.au/uncategorised/a-surgeons-very-real-concerns-about-my-health-record/>

engage the ALRC to conduct an inquiry into the legal accountability of AI-informed decision making (Proposal 3). We would also welcome additional reviews that place greater public scrutiny on AI-informed and automated decision-making processes in consumer contexts to facilitate greater overall visibility and civil society awareness of predatory or discriminatory behaviours and pricing models. This level of visibility could also promote greater reflection within markets regarding their level of comfort with business models built on these types of practices.

Inclusive design practice (addressed in Chapter 10 of the Commission’s Discussion Paper), is another means to improving civic participation, co-regulatory understanding, and consumer education. This is relevant for a broad range of consumer technologies, including many that are being driven by AI. Inclusive design approaches not only create products that can improve individual experience, but also have a part to play in addressing structural issues, including gaps in existing consumer law approaches which “do not necessarily prompt a proactive response for supporting consumers with cognitive disabilities in building the capacity to make meaningful market-place decisions”³¹.

Human rights-based legal research suggests consumer protection for people who require decision-making support would be strengthened by shifting from “safety-net” consumer protections situated within a disability or vulnerability model (such as contractual release on grounds of lack of genuine consent) to a social model that provides legal protection for participation and access to goods and services. The aim of this approach is “to build expertise and tools for wider industry participation in supporting people with disabilities to be fully included as economic actors, as well as building informal supporters’ and specialist agencies’ capacities to provide this support”³².

CPRC supports further exploration of how regulatory sandboxes, such as ASIC’s FinTech sandbox³³ or the UK Information Commissioner’s Office data protection sandbox³⁴, might be used to enhance inclusive design of rights-informed AI systems and other data-driven technologies. We welcome further engagement with the AHRC regarding key features required of regulatory sandboxes to test AI-informed decision-making and algorithmic bias (matters outlined in Proposal 15 and Question F of the Commission’s Discussion Paper), and look forward to how our existing partnership with the AHRC, Data 61 and the Gradient Institute might continue to assist in this process.

2. Principles for a coordinated technology policy framework

CPRC suggests a coordinated data protection and management policy framework guided by clear platform-neutral and technology-neutral principles that remain applicable across sectors and services. This approach is vital to combating a fragmented policy environment that complicates organisations’ understanding of their responsibilities, hinders the ability of regulators to effectively enforce consumer protections, and confuses consumers’ comprehension of their rights.

31 Maker, Y., Paterson, J.M., Arstein-Kerslake, A., McSherry, B. and Brophy, L. (2018) ‘From Safety Nets to Support Networks: Beyond ‘Vulnerability’ in Protection for Consumers with Cognitive Disabilities’, *UNSW Law Journal* 41(3).

32 Ibid.

33 <https://asic.gov.au/for-business/innovation-hub/fintech-regulatory-sandbox/>

34 <https://www.govtechreview.com.au/content/gov-digital/article/uk-s-ico-selects-participants-for-sandbox-beta-1507078179>

We agree with the Commission that more needs to be done to ensure a coordinated approach to technology policy in Australia, a position also expressed in our formal submission to the ACCC Digital Platforms Inquiry³⁵. Our research report, *A Day in the Life of Data* (2019) further expands on the need for greater policy coordination at Federal level to establish policy responses that are both integrated and adaptable. As the AHRC Discussion Paper makes clear, policy responses to questions of human rights and technology intersect across a number of arenas. These include human rights law, but also privacy, discrimination, competition and consumer protection laws. Our view is that consumer rights are complementary to human rights, and both frameworks should deliver clear and lasting protections.

CPRC research has identified a number of areas where priorities for human rights and consumer rights in technology are co-indicated. These form the basis for six broad principles as discussed here, which we propose could usefully inform future policy interventions. We note there are both implicit and explicit overlaps between these principles and those presented by the Commission as necessary for accountable AI-informed decision-making (Chapter 6) and accessible technology (Part D).

2.1 Transparency – visibility over drivers, triggers, and disclosures in data collection and use

Transparency is fundamental to building trust, introducing accountability and enabling individuals to make informed choices and decisions about their activities in the digital age. However, research continues to highlight ongoing issues of opacity for service users regarding the volume and scope of personal data being extracted through provision of digital services, with a common example being the delivery of advertising via online platforms. Here, the collection and manipulation of user data by mediating platforms is not made clear to parties on either side of the equation: consumers are subject to information asymmetries that undermine their ability to make genuine choices (and to accurately assess whether use of such platforms and the services they promote align with their personal privacy preferences); while client advertisers do not have clarity over factors influencing the display of their advertising.

The need for transparency extends beyond advertising markets and online consumer aggregators. Many services necessary to participate in everyday society (including banking, communications, welfare, and taxation) now require the majority of interactions to be transacted through digital means, while innumerable others nudge consumers toward online options as a matter of ‘convenience’. It is rare for any of these services to offer full and proactive disclosures about how data is being collected, processed, shared or on-sold as a consequence of using services. The opacity of privacy policies and terms of service across the board, the lack of bargaining power available with regard to accepting these terms, and the implications of this with regard to consumer rights and agency are treated at length in our research reports *Consumer Data and the Digital Economy* and *A Day in The Life of Data*.

CPRC research also highlights that greater transparency of the data supply chain is required if policy makers and regulators are to design effective and fit-for-purpose interventions. One of the major challenges globally with regulation of data-driven technologies is that the ecosystem itself is not well understood, with expertise and market power being consolidated amongst a relatively small number of

35 Solomon, L. (2019) *Submission by Consumer Policy Research Centre to Australian Treasury consultation on the ACCC Digital Platforms Inquiry Final Report* https://cprc.org.au/wp-content/uploads/DigitalPlatformsInquiry_CPRC2019_Final-1.pdf

large players. Many jurisdictions have voiced concerns about such players effectively creating data monopolies out of their users' data that not only compromise the privacy and economic rights of users, but also, through network effects and other factors, place extremely high barriers to entry of new players into those markets³⁶. Transparency over, and effective regulation of, the ownership of data is a key factor in ensuring fair and competitive digital services and markets; and governments require clear understanding of these new supply chains in order to assess and manage the social and economic impacts of associated technologies.

A principle of transparency supports cohesive policy frameworks by acting as a deterrent for predatory or unethical data practices; helping to prevent excessive concentrations of market power; and providing one precondition for meaningful consumer participation.

Transparency is an important principle for many of the Proposals set out in the Commission's Discussion Paper. Of these, we highlight Proposal 5 as being of particular significance for consumer rights: *The Australian Government should introduce legislation to require that an individual is informed where AI is materially used in a decision that has legal, or similarly significant, effect on the individual's rights*. As with the Commission's proposed definition of AI-informed decision making (noted at section 2.5 of this submission), we suggest that 'similarly significant' effects would include those that affect a person's access to essential services such as energy, telecommunications, basic banking services, and housing.

2.2 Understandability – comprehensibility of information and processes

Recognising that transparency alone is not enough to secure consumer agency or informed consent, a principle of *understandability* seeks to ensure that people using digital technologies and data-driven services are in a position to comprehend what information that is provided to them about those platforms and services means in practice. This might include:

- understanding the extent, purpose, movement, and products of any data being captured (and the degree to which data collection is achieved through overt user input or covert harvesting derived from online activity);
- comprehending terms of use and/or participation, including provisions for the acceptable scope and notification of any changes to such agreements and processes relating to the termination of agreements;
- knowing where such agreements transfer ownership rights over a person's data (including biometric data), intellectual property, or digital assets, or otherwise have power to affect their future access to essential and important services or exercise of legal rights; and
- apprehending future consequences that may be attendant on using the technology.

The extent to which information is comprehended is a key factor in determining successful attempts to improve the efficacy of disclosure requirements placed on businesses. Consumers tell us it is not only a lack of disclosure regarding technology mechanisms and data processes that prevents engaged participation and informed decision-making, but also the manner in which such information is made available when it is supplied. For example, consumer research conducted by CPRC in 2018 found that

³⁶ Zuboff, S. (2019) *The Age of Surveillance Capitalism* New York, Hachette Book Group.

94% of those surveyed hadn't read all of the privacy policies that applied to their activities in the preceding 12 months. Typically, users indicate they do not read such documents because they are lengthy, difficult to comprehend, difficult to locate, and because the cost-benefit ratio of the associated effort is perceived to be too high³⁷.

In order to counter disengagement from processes and policies affecting their lives, consumers of data-driven products and services should have access to readily understandable information about the purposes and outcomes of engaging with these technologies, whatever sphere of social or civic life they are occurring in. An obligation to ensure consumer comprehension should be placed on companies and entities producing or providing these products and services: individuals should not be expected to bear the full burden of interpreting complex documentation in order to know how and where their data is being handled, who is being given access to information about them, or whether automated decision-making is being used to determine significant aspects of their life path.

A principle of understandability supports cohesive policy frameworks by minimising and mitigating information imbalances; promoting social and economic literacies regarding the conditions and effects of data-driven interactions; and enabling more nuanced risk assessment and decision-making. As well, policy commitments to understandability have specific significance for protecting the rights of children, persons with cognitive disability and/or requiring support in decision-making, and third parties whose data may be exposed through another person's interaction with data services.

While emphasising the wider relevance of this principle, we suggest it is also of direct import to Proposals 7, 8 and 9 of the Commission's Discussion Paper, which together target the need for AI to be designed in ways that ensure comprehensible explanations (both technical and non-technical) can be provided by AI-informed decision-making systems or their designers to account for decisions produced by these technologies.

2.3 Agency – capacity for individuals to exercise control in systems interactions

The principle of *agency* operates from the premise that consumers should have capacity and opportunity to exercise control in their market interactions and choices. CPRC considers data rights are integral to consumer agency. These rights span multiple issues including data privacy, portability, erasure and disclosure.

Fundamental to agency is the question of consent. In CPRC studies, we have repeatedly heard that Australians do not feel they are provided with knowledge or bargaining power sufficient to exercise meaningful consent in how their data is being used. Individuals in consumer focus groups have reported frustration, angst and an overall sense of disempowerment in relation to their reliance on digital interactions where the terms of engagement are non-negotiable³⁸. The CPRC position, as stated in prior public submissions, is that consent to data practices must be voluntary, express, informed, specific to purpose, time-limited, and easily withdrawn.

³⁷ CPRC (2018) *Consumer Data and the Digital Economy*, p30.

³⁸ Ibid.

For example, CPRC has consistently recommended that consumers be given the right to erase their personal information and data, beyond the right to have factually incorrect information amended or deleted. This is fundamental to addressing the current power imbalance where, without capacity to require their data be deleted, consumers are placed in a weak bargaining position with regard to asserting control over the value and usage of their data. We believe that consumers who sign up to a service anticipating that their data is not of high value should have protection to adjust that assessment over time in accordance with changes to technologies and processing capabilities. Erasure rights offer consumer protection against large companies' ability to unfairly speculate and capitalise on the value of human data by account of their insider knowledge of technology assets and trends. Providing for increased agency over the erasure of data recognises the right of individuals to change their consumer behaviours in light of new knowledge or changing life circumstances. As well, without the specific right to erase data upon leaving a service, consumers are exposed to an unnecessarily heightened likelihood of data breaches, fraud, and scams due to inability to reduce the volume of personal information available about them that exists in the digital ecosystem. This presents unacceptable risk for individuals, and an added cost to business.

Data erasure is often closely linked to data portability. In addition to clear minimum protections for safety and privacy, for firms to be forced to compete to produce higher-quality privacy products and services, consumers must be able to access their data and be in genuine control over that data. Consumers need to be confident in their ability to freely transfer data away from a previous provider to enter into a new contract with a firm that better meets their needs and preferences. Again, we emphasise the role of this principle in ensuring protection for persons to make appropriate decisions about their data relative to a point in time. The Consumer Data Right introduced by the Australian government in 2019, if implemented effectively and with adequate protections, may provide Australians with more agency over their data by providing portability rights over consumer banking, energy and telecommunications data. This includes providing consumers a right to require that companies delete their CDR data if they are no longer comfortable with a company holding it where there is no other legal impediment to doing so.

Internationally, erasure and portability rights are specifically articulated in the EU's General Data Protection Regulation (GDPR), as part of a suite of rights aimed at providing greater agency and protection to individuals in relation to their personal data. Erasure rights (often referred to as 'the right to be forgotten') are established in Article 17, which provides data subjects with the right to have their personal data deleted or removed, within the scope of prescribed circumstances and limitations. Data portability is the subject of Article 20 of the GDPR, under which data subjects have the right to receive their personal data in a structured, commonly used and machine-readable format, and also to have that data transmitted to another controller where technically feasible (interpreted on a basis of reasonable systems interoperability rather than an obligation for controllers to achieve direct compatibility).

Essentially, Article 20 is intended to better enable data subjects in having the freedom to switch service providers without losing the information they have provided and created about themselves. However, like the right to erasure, the scope of this right has limitations. Specifically, it applies only to personal data that have been provided by the data subject, processed by automated means, and where this processing is based on either consent or contract. This illustrates the holistic nature of the GDPR and comparable instruments. Without parallel protections to ensure transparency and

understandability, this last provision could, for example, be weakened by its exemption of data generated through profiling activity allowable under opaque terms of contract.

CPRC strongly encourages narrow interpretation of any exemption of a right to delete for the purposes of exercising a contract. Given that many exploitative business models are established on the back of monetising personal information and data, contract provisions that require collection and processing of data for behavioural advertising or analytics (for example) should not be exempt from consumer rights to erase and/or port their data. By way of comparison, the California Consumer Privacy Act takes a more aggressive approach toward data brokerage than the GDPR, articulating the specific right of consumers to opt out of sale of personal information that a company might collect, retain, or disclose about a consumer (in addition to access/portability and deletion rights), and mandating that the opportunity to exercise such right should be clearly signposted by website operators through an “opt out” link on the primary landing page of their business.

Agency is fundamental to effective market competition and consumer wellbeing, a position confirmed in relation to the changing technology landscape by the final report of the ACCC Digital Platforms Inquiry³⁹. More broadly, the scope for consumer data exploitation emergent from our new environment of bundled technologies, data profiling, and algorithmic decision-making also raises serious societal questions of political manipulation⁴⁰ and the entrenchment of structural discrimination⁴¹. Community expectations are clear in this regard: urgent reforms are required to provide greater visibility, choice, and control with regard to the collection, dissemination and use of consumer data.

A principle of agency supports cohesive policy frameworks as the lynchpin around which many other protections coalesce. Establishing a rights-based regulatory context with a requirement for people to be able to make meaningful choices about privacy, profiling, and ongoing uses of their data for public and private benefit is important for building civic and consumer trust (and acceptance rates for data-driven public technologies); and acting as a strong motivator for companies to prioritise development of technologies and business models that are premised on robust and ethical data practices.

A number of the Discussion Paper’s proposals (such as those dealing with accessible technology) are likely to make an overall contribution to building environments in which people are able to exercise greater agency in data use and more direct control over their systems interactions. As well, from a consumer rights perspective, Proposal 4 (*the Australian Government should introduce a statutory cause of action for serious invasion of privacy*) may enhance consumer agency to challenge organisations that hold and process their data by providing protections against significant data-based invasions of privacy, and simplifying the case they are required to prove where data privacy has been significantly infringed.

39 ACCC (2019), *Digital Platforms Inquiry Final Report*, p22.

40 Tilburg Law and Economics Center (2018) *Shaping competition policy in the era of digitization*, Tilburg University, Netherlands.

https://ec.europa.eu/competition/information/digitisation_2018/contributions/tilburg_law_and_economics_center.pdf

41 Newman, N. (2014) *How Big Data Enables Economic Harm to Consumers, Especially to Low-Income and Other Vulnerable Sectors of the Population* https://www.ftc.gov/system/files/documents/public_comments/2014/08/00015-92370.pdf

Consumer agency in systems interactions – including meaningful consent, measures of control over how personal data is supplied and used, and the ability to challenge actions and decisions that are perceived to be unfair or incorrect – can support human rights outcomes in areas where such rights might otherwise be impinged. The case studies outlined at page 68 of the Discussion Paper provide pertinent examples here. As well, technology may itself supply functional agency for the exercise of human rights, as in the case studies at pages 156-157 of the Discussion Paper. Economy-wide policy responses that improve agency in consumer contexts by addressing power imbalances and providing protections for data rights can play an important role in improving human rights outcomes more widely, establishing frameworks that may be applied to uphold the rights of (among others) women, people with disability, and Indigenous peoples to exercise financial freedoms and self-determination.

2.4 Accessibility – equity in provision and application of technologies

Accessibility speaks to universal human rights to freely participate in a fair and equal society. In digital markets, these rights are compromised by the existence of divides in society that present barriers to online participation and prevent benefits of the digital economy from being shared equally. In Australia, this gap is acknowledged and monitored by measures such as the Australian Digital Inclusion Index. The Index's 2018 report explains its rationale:

Digital inclusion is based on the premise that everyone should be able to make full use of digital technologies – to manage their health and wellbeing, access education and services, organise their finances, and connect with friends, family, and the world beyond⁴².

Championing and monitoring a commitment to accessibility through the promotion of inclusive design methods and technology development that incorporates rights by design is one way to narrow this gap. As technology progresses, policy interventions must ensure these advances remain fair and accessible; rather than increasing conditions of inequality whereby those who face known vulnerabilities in the marketplace continue to obtain less access to (and benefits from) digital tools, platforms, and information to assist them in navigating markets than do already advantaged consumers.

Inequities play out in digital and technology-enabled consumer markets in a number of ways, including: local availability of products or infrastructure (such as access to reliable, or any, broadband network services); the capacity of individuals to participate in particular market opportunities (often limited on a financial basis); and the functional accessibility of products, services and websites. As noted by the Commission's Discussion Paper, functional accessibility affects people experiencing a wide range and combination of factors which may include physical or cognitive impairments; age, language or cultural barriers; low levels of digital literacy; or other circumstances that exacerbate digital exclusion if inadequately catered for in design and implementation of technology. Conversely, good design can bring opportunity and reward in the place of digital marginalisation. For example, sponsored research conducted by PwC in 2019 on behalf of the Centre for Inclusive Design

42 Thomas, J., Barraket, J., Wilson, C.K., Cook, K., Louie, Y.M., Holcombe-James, I., Ewing, S., and MacDonald, T. (2018) *Measuring Australia's Digital Divide: The Australian Digital Inclusion Index 2018*, RMIT University, Melbourne, for Telstra. <https://doi.org/10.25916/5b594e4475a00>

extrapolated that over 4% of Australians experiencing financial exclusion gained financial independence as a result of inclusively designed and targeted financial services⁴³.

Lack of diversity at the technology design stage is recognised as contributing to adverse consequences with regard to automated and AI-informed decision-making outcomes⁴⁴. The potential for algorithms to exhibit (and AI to learn) the biases of programmers and training datasets, leading systems to impose direct or indirect discrimination onto decisions informed by subsequent data, is demonstrated by case studies included in the Discussion Paper⁴⁵. We support the Commission's suggestion that this can be addressed, in part, through Rights by Design approaches and associated policy measures such as those suggested in Discussion Paper Proposals 13, 25, 26 and 27.

Cases where algorithmic bias has manufactured systematic discrimination in the programmatic outcomes of automated systems are well reported and disturbingly common⁴⁶. Drawing attention to such bias through public reporting and information programs has not proven to be a strong enough antidote: greater accessibility and inclusion measures within the education, research, and employment markets that serve as feeders for technology development are required to ensure perspectives reflecting the diversity of society have direct input at all levels of design processes (i.e., not just as research participants, design testers, or subjects of training datasets that may have been compiled with bias and without recognition of data rights).

*Much like the way we increasingly wish to know the place and under what conditions our food and clothing are made, we should question how our data and decisions are made as well. What is the supply chain for that information? Is there clear stewardship and an audit trail? Were the assumptions based on partial information, flawed sources or irrelevant benchmarks? Did we train our data sufficiently? Were the right stakeholders involved, and did we learn from our mistakes?*⁴⁷

If transparency is contingent on a paired principle of understandability to be an effective policy driver, agency is similarly contingent on the principle of accessibility. Accessibility facilitates cohesive policy reform by recognising and valuing diversity of experience, expertise, and knowledge as a necessary input into creating functional policy, fair markets, and holistic social systems. Where accessibility and relevant diversity of thought and experience are evident in design, or are perceived to be genuinely contributing to data policy and program initiatives, this also has downstream effects for enhancing consumer belief and participation in achieving the types of products and reforms that they desire from an inclusive society.

43 PwC (2019) *The Benefit of Designing for Everyone*. Centre for Inclusive Design. (Report sponsored by Adobe and Microsoft) <http://centreforinclusivedesign.org/media/1186/inclusive-design-report-digital-160519.pdf>

44 West, S.M., Whittaker, M. and Crawford, K. (2019). *Discriminating Systems: Gender, Race and Power in AI*. AI Now Institute, NYU <https://ainowinstitute.org/discriminatingystems.pdf>

45 AHRC (2019) *Human Rights and Technology Discussion Paper*, Australian Human Rights Commission; p68.

46 Eubanks, V. (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, St Martins Press/McMillan.

47 Etlinger, S. quoted in Rainie, L. and Anderson, J. (2017) *Code-Dependent: Pros and Cons of the Algorithm Age* <https://www.pewresearch.org/internet/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/>

While the Commission's 'Accessible Technology' proposals particularly acknowledge the requirements of people with disability, we note that several proposals in this section are similarly applicable to other cohorts and consumer groups who may experience structural, cognitive, or physical barriers to digital inclusion.

Specifically, we draw attention to Proposal 24 and Question G as having scope for expansion into aged care contexts and the rights of consumers in this sector. The internet is an increasingly essential service for this cohort in light of the online delivery of My Aged Care information about home care; the rapid growth of telehealth products and services in assisted living and aged care facilities⁴⁸; as well as its function for supporting the human right to retain connection to family⁴⁹.

2.5 Accountability – data holders and service agents are answerable for decisions and actions

Accountability requires all agents, especially decision-makers and those in positions of power, to be answerable for their decisions and role in events; to be able to supply the reasons and evidence for their decisions and actions; and to accept responsibility and atone for errors.

The Commission's Discussion Paper highlights a number of key issues in relation to ensuring accountability where an AI system is the primary decision-making agent, or heavily influences the actions of a human decision-maker (captured as Proposal 3 and Proposals 5-10). We share the Commission's concern regarding difficulties in determining causal effect or assigning human responsibility where AI-informed systems make, or contribute significant input into, decisions, and the implications for contestability and exercise of rights where these decisions have adverse outcomes for individuals. CPRC agrees that knowledge of when AI is materially used in decision-making that has legal or similarly significant effect on rights of an individual, as well as explainability of systems in language that can be understood by expert and non-expert humans, is a vital part of ensuring accountability of those systems.

In addition, we wish to draw attention to the rapid growth of intermediary businesses along consumer supply chains, their impact on advice and recommendations provided to consumers, and the associated implications for accountability. As more providers emerge between consumers and suppliers, more data is created along the supply chain. This can be used in socially beneficial ways, such as greater transparency of ethical supply chains or assisting consumers to more efficiently identify products that match their preferences. However, the data collected by transactional intermediaries is itself a valuable commodity.

Comparison websites, umbrella marketplaces, search and matching sites, some new mobile payment technologies, and online booking systems all have power to influence consumer behaviours, purchase decisions, and the types and uses of data collected about individuals who visit and use these third-party services. This is a structural change in markets that creates gaps in existing regulation, monitoring and accountability measures. Industry-specific regulations pertaining, for example, to the

48 Australian Aged Care Industry Information Technology Council (2020) *Submission to the Royal Commission into Aged Care Quality and Safety Consultation Paper 1*. <https://agedcare.royalcommission.gov.au/submissions/Documents/read-consultation-paper-1-submissions/AWF.660.00116.0001.pdf>

49 Provided for under Article 16 of the Universal Declaration of Human Rights.

display of pricing information often only apply to licensed retailers within those markets with no such regulatory oversight in place for the way pricing information may be presented or compared by other parties.

CPRC has particular concerns regarding the practice of data profiling by intermediaries. While the credit reporting system, for example, is held accountable through legislation and rules that govern how and when credit information can be used, the data brokerage system is not accountable in the same way. This limits the rights of consumers to challenge decisions made about them by companies controlling such data, including where these decisions may influence their ability to access essential services or other products and services that are of significant impact to quality of life.

We strongly encourage the principle of accountability be applied by policymakers to enable access by consumers to transformed data, particularly profile and scoring data that has been developed using their personal information and activity data. To support equitable markets, businesses should be answerable to individuals who are denied services (or are charged higher prices), in order that those consumers have recourse to contest decisions, correct flawed data, or modify their behaviours to obtain better deals, where this is possible and equitable. Without such protections, it is likely that companies will continue the existing practice of denying consumers visibility over profiling data on the basis that the process of aggregating and transforming this data render it as part of their commercial intellectual property.

A principle of accountability supports cohesive policy frameworks by demanding systems and processes remain explainable and traceable at a level of human comprehension, securing an evidence base and identifiable chain of responsibility to ensure visibility and oversight of data flows, manipulation and trafficking. This is important for developing and enforcing policy protections at micro levels (such as the individual's right to contest and obtain human review of legally significant decisions implemented on the basis on automated decision-making, including data profiling, as is provided for under Article 22 of EU's GDPR) as well as at macro levels, where cross-jurisdictional data flows and offshore data holdings currently contribute to regulatory grey areas.

The need for accountability in technology design and use is a strong theme in the Commission's Discussion Paper, albeit heavily directed toward the use of AI-informed decision-making systems (Proposals 3, 6, 7, 8, 10, 17 and 18). While we emphasise that AI is not the only site where greater accountability is needed to protect human and consumer rights as they are affected by the use and regulation of data-driven technologies, CPRC broadly supports the Commission's commitment to greater accountability in this field and endorses the Commission's proposed definition of AI-informed decision-making. We note our position that 'similarly significant' effects would include those that affect a person's access to essential services such as energy, telecommunications, basic banking services, and housing.

2.6 Sustainability – short term impacts do not compromise long term conditions/outcomes

Sustainability as a principle provides for long-term vision and a triple bottom line perspective regarding the use and effects of new technologies. Human rights comprise a significant element of sustainability

principles, however a sustainable approach also recognises that these rights co-exist alongside the requirement for economic and environmental protections.

Ensuring that growth in AI and data-driven technologies is sustainable and deployed in line with community expectations is critical to fostering ongoing economic and social benefit from these innovations. We strongly encourage support and investment from policymakers to enable independent research and civic participation that can provide insights to identify and facilitate human, environmental, and economic needs from new technologies across a longer timespan than is customary in many software development approaches and hardware design strategies.

For example, a significant sustainability issue from both consumer and environmental perspectives is in-built obsolescence limiting the lifespan of many technology products. An estimated 45 million tonnes of electronic waste is generated every year, a high percentage of which is disposed of as general waste, ending up in landfill and open tips, with the presence of heavy metals and other manufacturing elements creating ongoing hazards for the health of people, animals and plants. Nor does e-waste recycling offer an adequate solution to the issue, with similar health risks arising from crude and uncontrolled processing techniques that are commonplace in many jurisdictions⁵⁰. Consumers who wish to prolong the active life of devices in order to minimise their contribution to this problem – or those who face financial, learning, or other constraints preventing them from keeping pace with artificially accelerated product renewal cycles – are stymied by the ability of industry to follow a deliberate design strategy of planned obsolescence.

Policy mechanisms and government funding schemes can be used to create environments that ensure local research and development markets for sustainable technologies create economy wide benefits flowing back to Australian consumers over the longer term. Robust oversight of such schemes is necessary to ensure they are used to stimulate research and development that is consumer relevant, directed toward products that are fit for purpose, and incorporating appropriate recognition of data rights.

A principle of sustainability plays a core role in cohesive policy frameworks by embedding consideration of the wider context and long term implications of technology and data markets at all stages of their design and implementation; and creating legal certainty for consumers in relation to their dealings with companies that promote socially or environmentally unsound practices.

We note that Proposal 11 of the Commission's Discussion Paper engages, in a very specific context, with the need to imagine and address extended and long term implications of technology; proposing that the Australian Government should introduce a legal moratorium on the use of facial recognition technology in decision-making of legal or significant effect until an appropriate framework is in place.

50 LaMonica, M. (2008) <https://www.cnet.com/news/study-e-waste-recycling-poisons-people-with-heavy-metals/>

3. Conclusion

Technology is currently moving much faster than policymakers and regulators are able to keep pace. During this period of rapid transformation, the scope for swift and significant consumer harm is escalated. We strongly recommend increased and ongoing government investment in proactive investigation and monitoring of digital and data-driven markets, and further development and enforcement of human and consumer rights protections. While human rights, privacy, and consumer advocates all have a role to play in assisting people to understand and uphold their rights, responsibility for legal safeguarding (and taking action against breaches) of these rights demands active involvement by nimble, coordinated and well-resourced regulators.

Responsible development and application of AI and other data-driven technologies has the potential to materially improve the experience of all Australians. However, this outcome is heavily contingent on how products and services using these technologies are designed, implemented, and monitored; and the efficacy of laws that govern their use.

CPRC welcomes ongoing dialogue with the AHRC about the intersections between consumer protection, data privacy, and human rights; and how this might lend itself to collaboration and capacity building to generate effective policy interventions and shared understandings across disciplines and sectors.

For further discussions regarding our research or this submission, please contact Emma O'Neill, Research and Policy Director, at emma.oneill@cprc.org.au or on (03) 9639 7600.

Yours sincerely,

Lauren Solomon

**Chief Executive Officer
Consumer Policy Research Centre**