Consumer Policy Research Centre

Level 14, 10-16 Queen Street, Melbourne, Victoria 3000

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

Submission to The Attorney-General's Department – Privacy Act Review – Discussion Paper

10 January 2022

Submitted online via https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/consultation/intro/

The Consumer Policy Research Centre (CPRC) welcomes the opportunity to contribute to the consultation on the Privacy Act Review – Discussion Paper.

CPRC is an independent, non-profit consumer research organisation. Our mission is to improve the lives and welfare of consumers by producing evidence-based research that drives policy and practice change. Data and technology issues are a research focus for CPRC, including emerging consumer risks and harms and the opportunities to better use data and technology to improve consumer wellbeing and welfare.

CPRC has a keen interest in how Australia's privacy protection framework can be reformed so it offers modern, robust protections that ensure Australian consumers, and our overall society, are better off as the Fourth Industrial Revolution[1] continues to gather speed. CPRC commends the Attorney-General's Department for its detailed review of the feedback on the Issues Paper and for proposing a privacy reform with thoughtful and consumer-centric options.

Below are CPRC's response to various questions/proposals in the Discussion Paper.

Part 1: Scope and Application of the Privacy Act

2. Personal information, de-identification and sensitive information

CPRC is supportive of the proposed broadened definition of personal information, which we believe will be fundamental to the effectiveness of the revised Privacy Act. Currently, the definition of personal information is limited to data that directly identifies an individual (e.g. name, address, age, date of birth, health records, phone number). However, personal information generated today is much more than that and the ubiquity of multiple sources of non-identifiable data collected and aggregated can easily assist in reidentification.

In practice, what types of information would the proposed definition of personal information capture which are not presently covered?

CPRC supports the proposed list of personal information examples in the Discussion Paper (i.e. identifiers such as a name, identification number, location data, online identifier, and factors specific to the physical, physiological, genetic, mental, behavioural (including

[1] World Economic Forum, "Fourth Industrial Revolution", (accessed November 2021), https://www.weforum.org/focus/fourth-industrial-revolution.

predictions of behaviours or preferences), economic, cultural or social identity or characteristics of that person). In addition to these, CPRC strongly proposes that technical data (e.g. IP addresses and device identifiers such as mobile phone/device ID numbers) to also be considered as a type of personal information. In CPRC's *2020 Data and Technology Consumer Survey*, 82% of respondents said they would be uncomfortable with unique mobile phone/device ID numbers being shared (the same level of concerned as sharing a home address and health information).[2] This reflects the extent to which, for many consumers, mobile phones are no longer simply functional communication devices but have become hubs and repositories for generating and storing extensive personal data. Consumers are worried about how the collection, use and disclosure of this information can present risks to their privacy. Ensuring such technical data is included within the definition of personal information in the Act will help to mitigate such risks. Failing to do so would be significantly out of step with community expectations and technological advancements.

In addition, for the purposes of future-proofing the reform, we encourage Government to apply a principles-based approach to the definition of personal information to cater of data points that beyond the above-mentioned. Currently, other points of data such as battery life, volume levels and phone storage capacity are also being used by advertisers to identify consumers' phones and the apps they may be using – all information that is then being used on how best to implement targeted advertising.[3] While doing so, terminology such as "reasonably identifiable" should also be removed to avoid ambiguity in the implementation of the law. It is critical that the reform doesn't create loopholes for consumer privacy to be violated through other use of data and information.

4. Small business exemption

Implementing fair, safe and inclusive privacy protections for customers and clients in a digital economy should be part of any business model, regardless of size, structure or type of business. Our *2020 Data and Technology Consumer Survey* revealed that 75% of consumers consider companies have the highest level of responsibility to provide protection against collection and sharing of personal information.[4] Given the increasing role of data collection, use and disclosure across the Australian economy – and the government's efforts to accelerate this trend – we remain firm that it is essential to extend the scope of the Privacy Act to more businesses by removing the small business exemption. This would be at par with other regulations that aim to protect consumers from the risk of harm, such as product safety mandatory standards and bans[5] which do not exempt small businesses from the expectation to keep consumers safe.

Creating limited rules or exemptions to specific Australian Privacy Principles (APPs) for small businesses, will only create more confusion amongst businesses on their expectations. For consumers, it will lead to disparity on how their personal information is protected across the digital economy, including in specific data sharing schemes. For example, as noted in the submission by the Financial Rights Legal Centre, recent amendments to the Consumer Data Right (CDR) rules enabling consumers to provide consent to disclose their data to "Trusted Advisors" would mean that such entities, which are often small businesses would fall under the current exemption and would not be expected to meet the same standards for collection,

[2] CPRC, "2020 Data and Technology Consumer Survey", (December 2020), https://cprc.org.au/publications/cprc-2020-data-and-technology-consumer-survey.
[3] The Washington Post, "When you 'Ask app not to track,' some iPhone apps keep snooping anyway", (23 September 2021), https://www.washingtonpost.com/technology/2021/09/23/iphone-tracking/.
[4] CPRC, "2020 Data and Technology Consumer Survey", (December 2020), https://cprc.org.au/publications/cprc-2020-data-and-technology-consumer-survey.
[5] See product safety mandatory standards and ban: https://www.productsafety.gov.au/product-safety-laws/safety-standards-bans.

use and disclosure of data. In these circumstances, the onus will once again be unduly placed on the consumer to understand the scale of the business and to determine what level of privacy protection would be offered to them. It also opens up the opportunity for bad actors to exploit this loophole under the guise of operating as a small company. Consistent and clear regulations across the sector can help reduce operational and compliance complexities.

How can small businesses be encouraged to adopt best practice information collection and handling?

We are supportive of OAIC's proposal to support small businesses with their compliance obligations, in recognition that small businesses do not always have access to the level of resources that would be available in a large organisation. However, for this level of support to be sustainable, Government should consider the provision of further resources for OAIC so it is well-equipped in supporting this cohort. We also note that, in addition to the OAIC, the Treasury may also be in a position to provide small business policy support and assistance. Given also its work on the CDR, including development of privacy principles within the CDR regime, there may be merit for the OAIC and the Treasury to work in partnership.

Part 2: Protections

8. Notice of collection of personal information

Standardised notices to support consumer comprehension

CPRC is supportive of introducing an express requirement that privacy notices need to be clear, current and understandable. We are also supportive of standardised layouts, wordings and icons to assist with consumer comprehension to reduce the burden on consumers. To achieve this, CPRC strongly encourages the Government to embed comprehensive consumer experience (CX) research as part developing standardised layouts, wordings and icons. The CX research should be thorough with statistically significant consumer samples and be representative of the Australian population, capturing varying levels of digital literacy and experience and including consumers experiencing vulnerability. This will assist to adequately measure the impact of the standardised content and its practicality in meeting consumer needs.

Comprehensive consumer experience (CX) research

Research should also measure consumer comprehension of rights and risks, and the implications of sharing their personal information in particular use-cases. Our *2020 Data and Technology Consumer Survey* confirmed that privacy policies continue to be ineffective in engaging Australians, as 94% of consumers report not reading such information all the time and 33% of consumers never read these documents at all. Of the 67% who had read terms and conditions at some point in the 12-month period, 69% reported accepting terms even though they were not comfortable with them, with the majority (75% of those consumers) accepting them as it was the only way to access the product or service.[6] Improvements to privacy policies and notices need to be able to address this reduced capacity to give informed consent and the lack of agency consumers currently experience over the choice of how their personal information is collected, shared, used and disclosed.

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

Strengthening proposal 8.2 on types of circumstances requiring notices

We support the types of information nominated for notices; however, requiring notice for the "*purpose(s) for which the entity is collecting and may use or disclose the personal information"*, does not effectively go far enough. CPRC recommends inclusion of a further notice type which specifically outlines how consumers' data will be used to influence or make predictions about them, or how their data is being shared with other entities (i.e. raw data or specific insights). Knowing this information will help enable consumers to make informed, meaningful choices on this basis. The Privacy Act needs to place a clear onus on businesses – in particular those whose business models are predicated on the collection, use and disclosure of consumer data – to satisfy themselves that consumers are being enabled to make informed, meaningful choices.

9. Consent to collection, use and disclosure of personal information

Are there additional circumstances where entities should be required to seek consent? Should entities be required to refresh or renew an individual's consent on a periodic basis where such consent is obtained for the collection, use or disclosure of sensitive information?

While CPRC is supportive of defining consent in line with GDPR and considering standardised consents to assist with consumer comprehension, we reiterate our concerns from our previous submission on the over-reliance on consent and choice in the absence of protections which ensure safe and fair treatment. Safety and fairness should not be left to consumer choice – these are things which consumers expect the law to ensure regardless of choice. Our research indicates that the proliferation of choice, while ostensibly a positive for consumers, has also led to an increase in frustration and confusion. Choice becomes meaningless and even detrimental if it is not structured in a way that is clear and easy for consumers to navigate and act in accordance with their preferences.[7]

10. Additional protections for collection, use and disclosure

Should the fair and lawful collection requirement in APP 3.5 be subsumed by an overarching fair and reasonable requirement, or should a fair and reasonable requirement apply only to purposes for use and disclosure in APP 6?

CPRC welcomes the introduction of the 'fair and reasonable' requirement and strongly urges that it be an overarching requirement within the Privacy Act, instead of being required for specific APPs only. In addition to this, we caution that even an overarching requirement in the Privacy Act would not negate the need for broader fairness reforms within consumer law, because unfair practices are not constrained to only privacy matters. As part of reforming the Privacy Act, we urge the Government to not delay the introduction of an unfair trading prohibition and the strengthening of unfair contract terms in consumer law to address the emerging range of unfair practices businesses adopt that are amplified in the digital age.

Would the proposed definition of a secondary purpose inadvertently restrict socially beneficial uses and disclosures of personal information, such as public interest research?

Defining 'secondary purpose' as, *"a purpose that is directly related to, and reasonably necessary to support the primary purpose",* narrows the scope of the data being used for socially beneficial uses. One option that the Government could consider is the development of a third tier (tertiary purpose) to clearly identify when personal information may be used for

[7] CPRC, "The Digital Checkout", (December 2021), https://cprc.org.au/publications/the-digital-checkout/.

socially beneficial uses such as public interest research. This can create a clear distinction between data that is used for a specific purpose that may relate to the experience of an individual or group of consumers and when data is part of a broader study. In defining these purposes, we continue to urge that any sharing arrangements, whether via open data or bespoke arrangements are undertaken thoughtfully, with 'fair and reasonable' tests and adequate safeguards in place.

11. Restricted and prohibited practices

Would the introduction of specified restricted and prohibited practices be desirable? Should restricted practices trigger a requirement for APP entities to implement additional organisational accountability measures, or should individuals be provided with more opportunities to self-manage their privacy in relation to such practices?

CPRC supports the introduction of specified restricted and prohibited practices to provide a fair and safe environment for consumers to confidently engage in the digital economy. We also welcome the proposal that these restricted practices trigger a requirement for APP entities to implement additional accountability measures instead of placing the burden on consumers to navigate settings and self-manage their privacy. CPRC holds the view that "Bounded Rationality" is the theory that individuals have a limited capacity to assimilate and digest all the information required to make perfectly rational decisions.[8] The concept plays a critical role in consumer choice behaviour and should be taken into account when considering the cognitive load on consumers who are already experiencing information overload within the digital economy.[9]

What acts and practices should be categorised as a restricted and prohibited practice, respectively?

As raised in our previous submission, CPRC considers there are certain kinds of data collection, use and disclosure practices that drive too much of a power imbalance or creates scope for discrimination and harm, particularly for minors or other people experiencing vulnerability. As a starting point, CPRC suggests that the Review prohibit data-handling practices that leverage the following types of personal information (either actual or inferred) in ways that have been shown to cause harm and discrimination:

- a person's emotional stress[10] or mental health circumstances[11]
- a person's physical health and likelihood of disease[12]
- a person's inexperience in a market and potential financial vulnerability[13]

In relation to restricted practices, CPRC is supportive of the list proposed in *11.1 – Option 1* of the Discussion Paper but would recommend the inclusion of behavioural tracking and profiling for the purposes of delivering personalised content (e.g. recommendations on

[8] See: Herbert Simon, "Models of bounded rationality", (Cambridge, MA, MIT Press: 1982). 64 Aleecia McDonald & Lorrie Cranor, "The cost of Reading Privacy Policies". (I/S: A Journal of Law and Policy for the Information Society 2008 Privacy Year in Review), 4(3), http://www.aleecia.com/authors-drafts/readingPolicyCost-AV.pdf
[9] CPRC, "Consumer Wellbeing Research", Unpublished research.
[10] Andrew Hutchinson, "On Facebook's Emotional Ad Targeting, the Manipulation of Younger Users, and the Concerns of Big Data", (May 2017), https://www.socialmediatoday.com/social-networks/facebooks-emotional-ad-targeting-manipulation-younger-users-and-concerns-big-data.
[11] ABC News, "Insurers gaining 'open-ended access' to medical records slammed as 'unfair privacy breach'", (January 2019), https://www.abc.net.au/news/2019-01-24/medical-records-handed-to-insurance-companies-over-mental-health/10720024.
[12] Phuong Nguyen & Lauren Solomon, "Consumer Data and the Digital Economy", (July 2018), https://cprc.org.au/publications/report-consumer-data-and-the-digital-economy/.
[13] Vivien Chen, "Online Payday Lenders: Trusted Friends or Debt Traps?". (UNSW Law Journal, Volume 43(2), 2020), 675, http://www.unswlawjournal.unsw.edu.au/wp-content/uploads/2020/06/10-VIVIEN-CHEN.pdf

streaming services[14]). Our *2020 Data and Technology Consumer Survey* found that 76% of consumers found it unfair or very unfair for their personal information being used to make predictions about them.[15]

CPRC also continues to strongly recommend that government undertake further research (with civil society and academia where appropriate) to establish what other kinds of data collection, sharing and use practices present significant risks of harm and discrimination to consumers. We would urge all parties to publish their research as quickly as possible to ensure the consultation on these key issues is fully informed.

Should prohibited practices be legislated in the Act, or developed through Commissioner-issued guidelines interpreting what acts and practices do not satisfy the proposed fair and reasonable test, following appropriate public consultation?

We recognise that getting the balance right will hinge on laws and regulations sending a clear signal to entities of what is expected in a range of data handling circumstances. For example, Canada's Personal Information and Protection and Electronic Documents Act sets an expectation that "*an organisation may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances*".[16] The recently revised Swiss Federal Act on Data Protection is another example where in allowing organisations to process data without consumer consent, there is an express requirement that the process cannot violate "*the personality of individual*".[17] Similar requirements in the Privacy Act could be a useful basis to set the expectation upfront in legislation, but where possible, Government should endeavour to embed prohibited practices into the legislation to ensure the severity of such practices is understood. In addition, principles relating to "proceed with caution" practices could be clarified via Commissioner-issued rules and guidance on what is expected in different circumstances.

12. Pro-privacy default settings

Should pro-privacy default settings be enabled by default, or should requirements be limited to ensuring that privacy settings are clear and easy to access? Should pro-privacy default settings be enabled by default, or should requirements be limited to ensuring that privacy settings are clear and easy to access?

As noted in our previous submission, CPRC strongly supports defaults for data sharing to be set to off (Option 1) to enable consumers to make active choices about disclosing their data. Pro-consumer defaults should also be supported by protections that mean firms cannot preclude access to a good or service if a consumer refuses to consent to the unnecessary collection of their personal information. While clear and easy-to-access privacy settings should be part of any good business model, ultimately any choice that is presented to consumers should not compromise fairness or safety or shift the onus of the decoding these concepts on to individual consumers.

Our *2020 Data and Technology Consumer Survey* revealed that 88% of consumers find companies requiring more information than is necessary for delivering a product or service to

[14] Anna Johnston, "Privacy law reform in Australia – the good, the bad and the ugly", Salinger Privacy, 3 December 2021, https://www.salingerprivacy.com.au/2021/12/03/privacy-act-reform-proposals.
[15] CPRC, "2020 Data and Technology Consumer Survey", (December 2020), https://cprc.org.au/publications/cprc-2020-data-and-technology-consumer-survey.
[16] Government of Canada, "Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)", (June 2021), https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html.
[17] PWC, "New Swiss Federal Act on Data Protection: 5 changes to remember", (Accessed: 7 December 2021), https://www.pwc.ch/en/insights/fs/data-protection-switzerland.html.

be very unfair or unfair.[18] It is also estimated that the average time spent using the internet (across all devices) is more than six hours a day[19] so expecting consumers to adjust privacy settings across all sites and platforms they access, places an undue cognitive load on consumers who are already experiencing a sense of feeling overwhelmed with the volume of information they are expected to digest to make informed choices.[20] By introducing pro-consumer defaults, consumers can be confident that the baseline settings on any digital platform are enabling fair and safe collection, use and disclosure of their data. Any modulation of those settings should be if the consumer chooses to widen the scope of data being collected, used and shared instead of narrowing it. This will result in giving consumers genuine agency and control over their choices.

If pro-privacy default settings are enabled by default, which types of personal information handling practices should be disabled by default?

Our research[21] has revealed that consumers consider the following common data practices to be unfair:

- Using personal information to make predictions about a consumer.
- Collecting information about consumers from other companies.
- Sharing personal information consumers have provided with other companies.
- Selling personal information consumers have provided to other companies.
- Requiring more personal information than necessary to deliver products/services.

Consumer trust is a fundamental building block in efficient markets.[22] Ensuring practices that create distrust are disabled will help to ensure consumers participate in digital markets. CPRC recommends that the above data practices should be disabled by default to ensure consumers are provided with a digital experience that is fair, safe and inclusive and to facilitate consumer trust in growing digital economy.

15. Right to erasure of personal information

In light of submitter feedback, should a 'right to erasure' be introduced into the Act?

As mentioned in our previous submission, CPRC strongly supports consumers being given the right to erase their personal information and data held by companies where there is not a legal reason for it to be retained. CPRC's *2020 Data and Technology Consumer Survey* found that 89% of consumers considered such a right to be fair (71% very fair, 18% fair). We also agree with the ACCC that a right of erasure is a critical complement to strengthened consent requirements because it provides consumers with a mechanism for withdrawing their consent if they are no longer comfortable with an entity collecting, using or sharing their personal information. Without any capacity to require their data to be erased, consumers are not in a strong bargaining position with businesses when it comes to the collection, sharing and use of their data. This is especially so when it comes to potential future uses of that data because the value of data changes through time with the technology that is applied to it.

---

[18] CPRC, "2020 Data and Technology Consumer Survey", (December 2020), https://cprc.org.au/publications/cprc-2020-data-and-technology-consumer-survey.
[19] we are social, "Digital 2021 Australia: We spend 10% more time online", (February 2021), https://wearesocial.com/au/blog/2021/02/digital-2021-australia-we-spend-10-percent-more-time-online/.
[20] CPRC, "Towards a wellbeing approach to consumer policy in Australia – Part One: Why now?", (November 2021), https://cprc.org.au/publications/towards-a-wellbeing-approach-to-consumer-policy-in-australia/.
[21] CPRC, "2020 Data and Technology Consumer Survey", (December 2020), https://cprc.org.au/publications/cprc-2020-data-and-technology-consumer-survey.
[22] The Ethics Centre, Trust, Legitimacy and the Ethical Foundations of the Market Economy, (2018), 4, https://ethics.org.au/trust-and-legitimacy/.

A right to erase would ensure consumers have the ability to have their data deleted if they suspect it is being used for a different purpose to what they had originally signed up for.

16. Direct marketing, targeted advertising and profiling

Should express consent be required for any collection, use or disclosure of personal information for the purpose of direct marketing? Should the unqualified right to object to marketing extend to the collection and use of personal information where it is aggregated with the personal information of other users for marketing targeted at cohorts rather than individuals?

Our consumer research continues to indicate the opposition consumers feel towards targeted advertising with 60% considering it very or somewhat unacceptable for their online behaviour to be monitored for targeted ads and offers.[23] CPRC strongly recommends that pro-consumer defaults where consumers actively opt-in instead of opt-out for targeted advertising and offers will give them genuine agency and control over their data. This will also ensure consumers, regardless of their digital literacy, can confidently reap the benefits of the digital economy. We also support consumers having the right to object to marketing where information is either aggregated with personal information of other users for marketing even if it is only targeted to cohorts or aggregated information is disaggregated for potential misuse. This leads back to consumers being at the centre of choice on how their data is collected, shared and used.

Do customer loyalty schemes offer more tangible benefits to consumers, and should they be regulated differently to other forms of direct marketing?

CPRC urges Government to avoid creating a tiered system within the Privacy Act reforms that enable exceptions to how consumer data is collected, shared and disclosed. Whether it's a loyalty scheme, a paid or free product or service, consumers deserve baseline safeguards on their personal information. The market power of companies engaging in loyalty schemes will further strengthen if there are exceptions or different standards applied to how customer information is managed through those schemes due to increased possibility of regulatory arbitrage. CPRC's *2020 Data and Technology Consumer Survey* found that 60% of consumers were uncomfortable with companies sharing their personal information with third parties for purposes other than delivering products and services they'd signed up for.[24] In its loyalty schemes review in 2019, the ACCC raised concerns on the opacity of data sharing that occurs with third parties via loyalty schemes and recommended that loyalty schemes should continue to take steps to address these concerns and improve the transparency of their data practices and the ability of consumers to control how their data is collected, used and disclosed.[25]

17. Automated decision-making

Currently the Discussion Paper only proposes that the privacy policy include information on whether personal information will be used in automated decision-making. We urge the Government to look beyond the notification model and consider specific safeguards in ensuring fairness and safety of consumers in the context of artificial intelligence. Algorithmic bias which can be inherently present in AI-powered decision-making tools can lead to unfair

[23] CPRC, "2020 Data and Technology Consumer Survey", (December 2020), https://cprc.org.au/publications/cprc-2020-data-and-technology-consumer-survey.
[24] *Ibid.*
[25] ACCC, "Customer loyalty schemes – final report", (December 2019), https://www.accc.gov.au/publications/customer-loyalty-schemes-final-report.

treatment and discrimination.[26] CPRC's research in partnership with the Australian Human Rights Commission notes that transparency (including via notification) is only one facet of promoting responsible business use of AI and data. In addition, principles such as accessibility, accountability, agency, understandability, explainability, and sustainability are critical to include in AI architecture that is set-up for consumer.[27] In particular, the principle of sustainability which is specific to considering long-term implications of such technology is paramount in ensuring fair, safe and inclusive practices.

Part 3: Regulation and enforcement

24. Enforcement

Which option would most improve the complaints handling process for complainants and allow the OAIC to focus on more strategic enforcement of the Act?

CPRC supports establishing a Deputy Information Commissioner – Enforcement to allow OAIC to have more dedicated focus on enforcement (Option 3). Effective and regular surveillance and enforcement by the regulator is needed to educate and shift the market towards a more consumer-centric approach to privacy. The onus cannot remain on consumers alone to identify and report breaches to the regulator after the harm takes places. To truly create an effective ecosystem for privacy protections, effective complaints mechanisms need to supplemented by an adequately resourced regulator with the capacity and capability to monitor and enforce privacy breaches in this complex environment.

As mentioned above, for the Privacy Act to be effective, in addition to well-resourced enforcement, there must be simple, accessible and effective dispute resolution pathways to enable consumers to seek redress for when things go wrong. In the 2016 Australian Consumer Survey led by Treasury, only 4 in 10 consumers were aware of dispute resolution services provided by consumer protection agencies.[28]

While CPRC supports consumer access to an ombudsman (Option 2), we are concerned with the issues-based approach that Government is taking to complaints handling for digital harms. For example, the ACCC has also recommended the establishment of an ombudsman scheme but only on issues relating to digital platforms.[29] An ombudsman scheme specifically on privacy issues further segments digital dispute resolution, placing the onus back on consumers to identify the type/s of digital harm they may have experienced through an incident and to then decipher which ombudsman to seek support from. In our recent Digital Checkout report, we recommend that Government finalise and release a scoping study as a matter of priority to identify the types of online disputes consumers are raising along with options for establishing more effective external dispute resolution pathways that not only address digital issues today but also complex matters that are likely to arise in the future.[30] As mentioned in previous CPRC submissions, we believe there may be merit in a more holistic approach to dispute resolution, such as via the establishment of a Digital Ombudsman that can provide support on all facets of a digital experience.

---

[26] Australian Human Rights Commission, "Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias" (2020), https://tech.humanrights.gov.au/downloads.
[27] *Ibid.*
[28] The Treasury, "Australian Consumer Survey 2016", (May 2016), https://consumer.gov.au/sites/consumer/files/2016/05/ACL-Consumer-Survey-2016.pdf.
[29] ACCC, "Digital Platforms Inquiry – Final Report", (July 2019), https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report.
[30] CPRC, "The Digital Checkout", (December 2021), https://cprc.org.au/publications/the-digital-checkout/.

26. A statutory tort of privacy

CPRC continues to support the Privacy Act reforms, recommended by the ACCC, regarding the introduction of a direct right of action for individuals and the introduction of a statutory tort for serious invasions of privacy (*26.1 – Option 1*). We consider both reforms will help to strengthen the rights and bargaining power of consumers when it comes to handling their data and exercising their right to privacy.

Further engagement

We would welcome the opportunity to work with Government and share further insights from our consumer research projects. For further discussion regarding our research and the contents of this submission, please contact me at **chandni.gupta@cprc.org.au.**

Yours sincerely

Chandni Gupta
Acting Chief Executive Officer
Consumer Policy Research Centre