Consumer
Policy Research
Centre

Submission

Safe and responsible AI in Australia – Department of Industry, Science and Resources

27 July 2023

About the Consumer Policy Research Centre

The Consumer Policy Research Centre (CPRC) is a not-for-profit consumer policy think tank.

Our work is possible thanks to funding from the Victorian Government.

Our role is to investigate the impacts that markets and policies have on Australian consumers and advise on best practice solutions. Consumer protections in the digital world is a current research focus for CPRC.

Contact for submission

Chandni Gupta
Deputy Chief Executive Officer + Digital Policy Director

Email: chandni.gupta@cprc.org.au

Submission made via: https://consult.industry.gov.au/supporting-responsible-ai

Statement of Recognition

CPRC acknowledges the Traditional Custodians of the lands and waters throughout Australia. We pay our respect to Elders, past, present and emerging, acknowledging their continuing relationship to land and the ongoing living cultures of Aboriginal and Torres Strait Islander Peoples across Australia.

Let’s make AI fair, safe and inclusive

AI and new technologies will continue to develop quickly. The Federal Government should focus on creating a legal and regulatory framework that ensures that when businesses use new technologies, including AI, that consumers are kept informed, treated fairly and not subject to unsafe practices.

The Federal Government must fast-track reforms for consumers in the digital economy to ensure Australians are protected from current and future harms. **Failure to strengthen consumer protections will mean businesses will be able to implement AI tools that make predictions that leave people worse-off, aggregate data that leads to exclusion or expose people’s vulnerabilities for commercial gain.**

The Federal Government must prioritise the following economy-wide reforms to deliver a holistic consumer protection framework that effectively holds businesses implementing AI accountable:

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

Implementing bespoke regulatory frameworks without adequate foundational economy-wide guardrails, will create a difficult to navigate system for consumers and a regulatory burden for businesses that have whole-of-organisation wide systems across multiple frameworks. It also creates the potential of regulatory arbitrage by rogue businesses.

In addition to these economy-wide consumer protections, some AI specific regulation is needed. At minimum, the Federal Government must require that businesses using AI clearly label when this is the case and disclose how it has been established. This transparency will provide a pre-condition for good consumer protection in future, helping regulators, researchers and the general public understand how the technology is being applied.

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

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

Our submission uses insights from CPRC’s research and considers the questions raised in the discussion paper using three key principles – fairness, safety and inclusivity for consumers engaging in the digital economy.

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

Question 2: What potential risks from AI are not covered by Australia's existing regulatory approaches? Do you have suggestions for possible regulatory action to mitigate these risks?

Australia's existing approach to consumer protection has major weaknesses. Our consumer law and privacy laws are very weak when compared with approaches in the EU, US, and Asia. Gaps in our laws need to be addressed to handle the risks of business use of AI to consumers as well as to stop harm overall. In this section we identify specific gaps in the Australian Consumer Law (ACL) and privacy protections that need to be addressed to create a holistic and technology-neutral consumer protection framework.

Implementing bespoke regulatory frameworks without adequate foundational economy-wide guardrails, will create a regulatory burden for businesses navigating whole-of-organisation wide systems across multiple frameworks. It also creates the potential of regulatory arbitrage by rogue businesses.

An example of this is the implementation of the Consumer Data Right (CDR). CPRC has continued to raise concerns of the bespoke privacy framework that currently operates within the CDR regime.[1] As CDR continues to expand data-sharing capabilities to entities outside of the CDR regime, it increases the risk of data misuse, data breaches, identity and material theft and reduced consumer rights, as rights under the CDR regime currently do not apply to data shared outside of the regime.

In developing any AI-specific regulation, the Federal Government must ensure consumers are afforded the same level of protections, no matter which part of the digital economy they engage within.

Data is the foundation of any AI system – it plays a critical role in how AI systems make decisions, draw conclusions and perform tasks. However, our research at CPRC confirms that there is **a grave mismatch between how businesses collect and use data and what Australians expect**:

- Only 15% of Australians feel businesses are doing enough to protect their privacy when it comes to how their personal information is collected, shared and used.
- Close to 60% of Australians have little to no confidence in online businesses (large or small) to keep their data safe.
- 83% believe personal information should not be collected and used in a way that harms them or others.
- Only 18% are confident that they will be compensated if they've been left worse-off because of how a company collected, shared or used their information.
- 70% believe personal information should only be collected or used if it is in a person's best interest and is unlikely to cause harm to them and others.

However, there are currently no safeguards in place to restrict businesses from implementing AI tools that:

- make predictions about people in ways that can leave them worse-off
- use and aggregate data to unfairly exclude people from accessing certain products and services
- target people to expose their vulnerabilities for commercially beneficial outcomes
- foster little transparency on what people are presented, what they consume and at what price, and
- lack adequate support for people seeking redress from AI-related harms.

The reason behind the mismatch is that whole-of-economy wide laws for consumer and privacy protections in Australia are currently inadequate in delivering safety and fairness that Australians expect and deserve. Australia must fast-track a range of economy-wide reforms to deliver consumer protections that Australians expect and citizens of other jurisdictions take for granted.

[1] CPRC, "Submission to Treasury: Consumer Data Right – Strategic Assessment", (August 2021), https://cprc.org.au/submission-to-treasury-consumer-data-right-strategic-assessment.

***Risk:** Businesses can use tactics or approaches that create deeply unfair outcomes for customers*
***Solution:** Introduce an unfair trading prohibition*

Unlike other countries that have prohibitions on unfair practices, business practices that lead to unfair consumer outcomes are currently not illegal in Australia. Examples include business models that:

- predicate on opaque business processes that undermine consumer autonomy
- thrive on profiting from exploiting consumer vulnerabilities
- fail to provide accessible and meaningful support to their customers.[2]

Often these unfair business practices target those consumers specifically experiencing vulnerability or disadvantage.[3]

As an example of a potential unfair practice, a hypothetical supermarket is implementing an AI pricing solution to offer different prices to customers based on their usage of the website and information the business purchases about their other behaviour online. In practice, this leads to people on very low incomes who don't use online shopping elsewhere being charged higher prices for essential items. Overall, this would create a very unfair outcome for a group of consumers. This kind of practice is not currently illegal but could be prevented by a well-targeted prohibition on unfair trading.

CPRC recommends that the Federal Government prioritise its work on introducing a prohibition on unfair business practices that protects Australians today and in the future. In the context of AI, a prohibition such as this could help abate poor AI implementation that leads to consumer harm. It can lead to businesses considering AI through a lens of fair outcomes for consumers and enable regulators to hold businesses accountable when they fail to do so.

Regulators overseas are already using their laws on unfair trading prohibition to investigate harms via AI within their jurisdictions. As an example, the US Federal Trade Commission is currently investigating OpenAI, the creators of ChatGPT, for engaging in unfair or deceptive practices.[4] It is able to do so through Section 5 of the Federal Trade Commission Act which specifically prohibits unfair and deceptive business practices – a law that the US has had since the 1930s.

CPRC has conducted a comparative analysis of laws that ban or restrict unfair practices across Europe, the United States, the United Kingdom and Singapore. We have outlined key lessons that Australia can learn from these jurisdictions when implementing its own unfair trading prohibition.[5]

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

- be drafted as a principles-based law but with specific guidance or an evolving a blacklist of unfair practices to give clarity to both regulators and businesses
- allow regulators to investigate and proactively enforce the law before widespread harm takes place
- have provisions in place for the law to evolve over time to address new and emerging unfair practices
- hold businesses accountable through penalties and enforcement action that effectively deter unfair business practices
- offer meaningful redress to consumers impacted by unfair practices
- quickly stop practices found to be unfair overseas from making their way to Australia, and

[2] CPRC, "Unfair Trading Practices in Digital Markets: Evidence and Regulatory Gaps", (March 2021), https://cprc.org.au/unfair-trading-practices-in-digital-market-evidence-and-regulatory-gaps-2/.
[3] CPRC, "Imagining an unfair trading prohibition – CPRC Spark Series Webinar", (September 2022), https://cprc.org.au/event/utpwebinar/.
[4] Kang, C., and Metz, C., "F.T.C. Opens Investigation Into ChatGPT Maker Over Technology's Potential Harms", (July 2023), The New York Times, https://www.nytimes.com/2023/07/13/technology/chatgpt-investigation-ftc-openai.html.
[5] CPRC, "How Australia can stop unfair business practices", (September 2022), https://cprc.org.au/stopping-unfair-practices.

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

Risk: *Consumer data can be collected and used in ways that causes harm*
Solution: *Reform the Privacy Act to bring Australia's protection framework into the digital age*

Our privacy law still relies on notification and consent as the primary means of protecting consumers. By forcing consumers into a situation where they "decide once" about whether to share their data but bear the consequences potentially for the remainder of their life is not a fair trade. This starkly contrasts with the knowledge and capability of firms to understand the value and potential use of data, including how it can enable AI systems.

This reliance on notification and consent means that businesses are practically able to collect significant amounts of data about their customers and use it in almost any way for any outcome. There is currently no protection against businesses embedding consent for personal information to be collected, shared and used (including aggregation with other data points) into long, complex terms and conditions. As an example, the increased use digital application tools in rental markets, where people have little to no choice with the agents they engage with, require significant amounts of sensitive personal information to be shared as part of the application process. Potential renters are not empowered to raise concerns with the use of third-party AI-enabled tools to score them and their eligibility to rent the property.[6]

At minimum, any reform to the Privacy Act should prioritise protections that go beyond notifying consumers how data will be used or seeking individual consent and require businesses to stop using data in ways that are highly likely to cause harm.

We urge the Federal Government to fast-track the revision of the Privacy Act 1988 and heed the concerns and proposals made by consumer representatives during the March 2023 consultation on how Australia's privacy protections could be strengthened. Specifically, CPRC urges the Federal Government to:

- modernise what it means to be identifiable to cover information obtained from any source and by any means
- implement genuine privacy by default measures instead of placing the onus on consumers to opt-out of settings that are not designed with their interests in mind
- require all businesses to assess and ensure how they collect and use data leads to fair and safe outcomes that are in the interests of their customers and the community
- empower the regulator to swiftly ban or restrict harmful practices that cause direct and clear consumer harms, and
- provide a clear pathway for redress when things go wrong.

[6] CHOICE, "At What Cost? The price renters pay to use RentTech", (April 2023), https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/choice-renttech-report-release.

***Risk:** Seeking redress rests predominantly with individuals*
***Solution:** Make consumer guarantees enforceable*

The discussion paper considers the applicability of the ACL to AI and specifically leans on consumer guarantees. We agree that the ACL will apply to business use of AI. However, businesses are currently not held accountable under the consumer guarantees framework. There are two key limitations currently present under the ACL:

- There are no specific obligations in consumer guarantees that relate to any form of software or technology embedded in products or its associated updates.
- There are no civil penalties and no pathway for a regulator to enforce consumer guarantees.

These limitations mean that the onus currently is largely on individual consumers to pursue a refund, remedy or replacement under the framework when things go wrong. Technically, a regulator can take legal action against business for failure to comply with the guarantees, but the courts can merely direct the business to offer the consumer the appropriate remedy. There is no option for courts to apply the multi-million-dollar penalties that can be applied for other breaches of the consumer law, such as when businesses mislead their customers.

Our research into consumer issues in Victoria confirmed that close to half of Victorians (42%) had experienced one or more consumer guarantee related issues.[7] **Currently it can be extremely difficult for consumers to pursue consumer guarantees with traditional, physical products; expecting them to navigate the framework to address the AI-related harms is next to impossible.**

The ACL must be revised to enable regulators to obtain pecuniary penalties of consumer guarantees to help incentivise compliance. Treasury has already consulted on draft reforms to introduce penalties for consumer guarantees. This work needs to be reprioritised to address current and potential future harms to consumers.[8]

***Risk:** Consumers lack access to help and support when something goes wrong, especially when they are dealing with a large, online platform*
***Solution:** Create a clear pathway to online dispute resolution*

Australians don't currently have a clear and accessible pathway to redress when it comes to many facets of the digital economy. There is no easy, independent way of resolving disputes in the online space.

When consumers are unable to resolve issues directly with a utility like an energy provider or telecommunications company, they have access to independent support for redress through an ombudsman. However, in the case of redress relating to digital services and technologies, this support is out of reach. Consumers are frequently left to navigate any form of recourse themselves or simply give-up.[9] For some complaints, consumers may be able to raise issues through state-level tribunals, but these processes tend to be difficult to navigate and take long periods.

An example of this is accessing a remedy when a product or service is purchased via an online marketplace. Currently there is a lack of clarify of how the ACL applies to these actors. The term supply in the *Competition and Consumer Act 2010*, is narrowly defined as, "…in relation to goods—supply (including re-supply) by way of

[7] CPRC, "Consumer issues in Victoria – Problems complaints and resolutions", (May 2023), https://cprc.org.au/vic-consumers/.
[8] See Treasury's Consultation Regulation Impact Statement on consumer guarantees: https://treasury.gov.au/sites/default/files/2021-12/c2021-224294-cgsicris_2.pdf
[9] CPRC, "Australian consumer in their own words", (June 2022), https://cprc.org.au/australian-consumers-in-their-own-words/.

sale, exchange, lease, hire or hire-purchase".[10] As online marketplaces consider themselves as only a 'facilitator of the supply' but not the actual supplier, it creates scenarios where consumers are often left with the burden to resolve issues with the third-party seller on their own. This is particularly the case when the seller is based overseas, so enforcing the ACL is not only difficult, but likely impossible. At this point, there is no ombudsman or other avenue of support available for a consumer to seek redress.

CPRC's 2023 national research confirms that Australians are confused about who can help them or where they can get redress if an issue arises with how their data is utilised:

- 50% of Australians do not know where to seek help if they have a problem with how a company collects, shares or uses their personal information.
- 46% of Australians do not know who to seek help from if they believe their personal information is being used in a way that's causing them harm.[11]

Several participants in CPRC's qualitative research conducted in 2021, specifically noted not pursuing redress options for products or services purchased online, as they felt the likelihood of being compensated was low. In absence of support, consumers are left powerless, with no pathway to compensation.[12] When you factor in the additional layer of harms that an individual may experience through an AI-enabled product or service, their sense of powerlessness will only magnify.

CPRC strongly recommends that the Federal Government finalise and release a scoping study as a matter of priority to identify the types of online disputes consumers are raising along with options for establishing more effective external dispute resolution pathways. This work should consider digital issues today and complex uses of technology, including AI, that are likely to arise in the future. CPRC has raised this issue over several Government consultations as we believe there may be merit in a more holistic approach to dispute resolution, such as via the establishment of a Digital Ombudsman that can provide support on all facets of a digital experience.

Risk: *Enforcement in Australia often happens after significant consumer harm occurs; there is very little focus on stopping obviously harmful practices before they reach the market*
Solution: *Increase regulator resourcing to enable proactive enforcement strategies*

Currently, traditional compliance and enforcement models often take place post harm, where a pattern of harm has been identified and reported either by individuals or community groups. Much of the onus remains on consumers to identify and report breaches after they have lost money or faced other life-altering consequences.

In the context of AI, this is an insufficient approach to consumer protection, as identifying the root cause of harm is often unclear for individuals who may not even be aware that bias, incomplete data sets, and inaccurate assumptions may have led to poor AI-enabled outcomes for them. With little to no transparency on how consumer data is collected and used, it is impractical to expect that an individual or a community group would be able to identify and report the potential of harm to a regulator for investigation.

Australia needs well-resourced regulators with the capacity and capability to monitor and enforce consumer protection breaches in the complex digital environment, including in AI. Regulators need to have the powers and tools to proactively uncover harm that is currently obfuscated.

[10] Competition and Consumer Act 2010, Retrieved from https://www.legislation.gov.au/Details/C2011C00003
[11] CPRC, "Not a fair trade – Consumer views on how businesses use their data", (March 2023), https://cprc.org.au/not-a-fair-trade.
[12] CPRC, "Consumer issues in Victoria – Problems complaints and resolutions", (May 2023), https://cprc.org.au/vic-consumers/.

CPRC recommends that the Federal Government strengthen the powers of the regulator so it can effectively stop harmful behaviour and practices before widespread harm occurs and restrict likely harmful practices while investigations take place. The Federal Government must ensure regulators are adequately resourced with the capacity and capability to monitor and enforce the law in this complex environment. It must be empowered to undertake proactive investigations. Regulators need powers to take enforcement action swiftly and independently.

CPRC consumer research confirms that Australians expect governments to protect them against data misuse (88%). Australians also believe that regulators should have a range of mechanisms to hold businesses accountable. These include having:

- enough staff and resources to investigate how companies collect, share, and use personal information (82% strongly agree or agree)
- the power to require businesses to pause and test data practices that may lead to harmful outcomes for people (80% strongly agree or agree), and
- the power to ban data practices that cause harm (81% strongly agree or agree).

As part of the review of the Privacy Act, CPRC has proposed a Privacy Safety Regime that mirrors similar reforms that exist either in the Australian financial market such as the product intervention power[13] or the provision of bans under the Australian product safety framework.[14] Both reforms are designed to deeply reflect on emerging issues and ascertain how consumers may be protected from foreseeable harms.[15] If implemented, it can be applied to AI systems as it would give the regulator to power to ban or pause data-enabled systems that have the potential to cause consumer harm.

As an example, if a privacy safety regime was in place today, it would have meant that some uses of facial recognition technology could have been restricted immediately as the Office of the Australian Information Commissioner investigated its use by Bunnings, The Good Guys and Kmart.[16] Instead, we are relying on the good faith of businesses to stop using this controversial technology, many of which are placing commercial benefits of AI over the safety and wellbeing of Australians. Stronger penalties can be an effective disincentive but only if they are backed with effective enforcement.

[13] ASIC, “RG 272 Product intervention power”, (June 2020), https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-272-product-intervention-power.

[14] ACCC, “About product bans”, (Accessed 10 November 2022), Product Safety Australia website, https://www.productsafety.gov.au/product-safety-laws/safety-standards-bans/product-bans/about-product-bans.

[15] CPRC, “In whose interest: Why businesses need to keep consumers safe and treat their data with care”, (March 2023), www.cprc.org.au/inwhoseinterest.

[16] CHOICE, “Kmart, Bunnings and The Good Guys using facial recognition technology in stores”, (July 2022), https://www.choice.com.au/facialrecognition.

Risk: *Mandatory standard making is a long, drawn-out process which means that known safety risks continue for many years*
Solution: *Increase regulator resourcing to enable proactive enforcement strategies*

The discussion paper notes that the ACL includes provision to make mandatory product safety standards for goods and services, which could be applied to AI. However, these standards are made by the Commonwealth Minister after long and arduous policy-making processes, often taking years. As an example, risk of button batteries to young children was identified more than a decade ago17 and the ACCC first released its national strategy to improve the safety of button battery products in 2016 but the mandatory standards were introduced in 2020 and finally came into effect in 2022.

Given the pace of any digital environment, especially the rapid pace of AI development, this is not a model that can be relied upon for timely and effective regulation as a means to protect Australians. Australia needs a general safety provision to ensure there is an upfront obligation to ensure that products and services are safe. This legal model, where goods and services have to be safe before sold rather than proved to be unsafe after the fact, is already in operation in a number of other comparable jurisdictions such as the United Kingdom and Canada.

A general safety provision needs to:

- provide strong, binding incentives for traders to prevent unsafe goods entering the market
- provide commercial advantage to traders that are already exercising due diligence, and ensuring products are safe, and
- improve the ability for regulation to take proactive action in relation to unsafe products.[18]

With such safeguards in place, it can hold businesses accountable to ensure the safety of consumers when implementing any AI-enabled product or service.

Question 5: Are there any governance measures being taken or considered by other countries (including any not discussed in this paper) that are relevant, adaptable and desirable for Australia?

Given the rapid pace of AI deployment, when considering regulatory frameworks specific to AI, the Federal Government must consider the aspect of ensuring tech-neutrality. The discussion paper notes AI regulatory frameworks currently present in both Thailand and the European Union. However, in both jurisdictions, the initial drafting of proposed AI regulation had to be reconsidered post the introduction and prevalence of ChatGPT.[19] It is a clear example of how regulation in this space needs to be focussed on fair and safe outcomes instead of the present technology itself. AI will continue to evolve, and any regulatory framework needs to be broad enough and principle-based to ensure it is not lagging behind technology.

[17] See first Australian safety campaign on button batteries released in 2012: https://www.accc.gov.au/media-release/button-batteries-a-little-known-risk and first global campaign released in 2014 via the OECD: https://www.oecd.org/science/button-battery-safety-awareness-week.htm.
[18] CPRC, "The Digital Checkout", (December 2021), https://cprc.org.au/the-digital-checkout/.
[19] Volpicelli. G., "ChatGPT broke the EU plan to regulate AI", (March 2023), Politico, https://www.politico.eu/article/eu-plan-regulate-chatgpt-openai-artificial-intelligence-act/

Question 9: Given the importance of transparency across the AI lifecycle, please share your thoughts on:

- where and when transparency will be most critical and valuable to mitigate potential AI risks and to improve public trust and confidence in AI?
- mandating transparency requirements across the private and public sectors, including how these requirements could be implemented.

While transparency is not the only answer to ensuring fair and safe outcomes for consumers, it is a starting point to enable practices within an AI system to be independently examined and scrutinised.

CPRC recommends that Federal Government incorporate obligations for transparency across three tiers:

1. **Pre-implementation**: through pre-market impact assessments and regulatory sandboxes to ensure there is ex-ante regulatory oversight that adequately probes the system for potential consumer harm before release.
2. **Throughout the lifecycle**: through regular system assessments and reporting, recognising that AI systems are dynamic, evolving over time.
3. **To consumers and the community**: via disclosures at point of use to consumers so there is adequate awareness that AI has been used to curate what they are viewing, experiencing, being offered etc.

While the first two tiers of transparency will help mitigate harm as early as possible and enable a proactive surveillance approach by regulators, the third tier of transparency will empower consumers to also play a role in probing the efficacy of fair and safe outcomes from AI. **You cannot challenge what you don't know. Consumers should be informed in a meaningful way so they can effectively report and seek redress if they believe that an AI-enabled outcome has left them worse-off.**

The Attorney-General, as part of the Privacy Act review, is also considering the requirement of notification where the use of AI is present. CPRC recommends that the Federal Government conduct thorough consumer testing to develop effective and meaningful notification models. Notification, however, is only a part-solution and is only practical where consumers have meaningful choice of products and services. It addresses only the transparency aspect of a safeguard. It must be leveraged with other safeguards through economy-wide reforms noted earlier and an obligation to act in consumers' bests-interests (covered in the next section).

Question 11: What initiatives or government action can increase public trust in AI deployment to encourage more people to use AI?

Safeguarding against algorithmic bias – going beyond transparency

CPRC urges the Federal Government to consider specific safeguards in ensuring fairness and safety of consumers in the context of AI. Algorithmic bias which can be inherently present in AI-powered decision-making tools can lead to unfair treatment and discrimination.[20] Transparency alone cannot be the only measure of compliance for businesses.

Emerging technologies featuring algorithmic decision-making have the potential of becoming embedded across all facets of a person's life over the coming years. It will be critical that a genuine effort is made to ensure Australians can clearly see, understand and trust how AI, including automated decision-making (ADM) systems are being used and what the benefits are to them.

CPRC's research in partnership with the Australian Human Rights Commission notes that transparency is only one facet of promoting responsible business use of AI and data. In addition, the following principles are

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

critical to include in AI and ADM architectures to ensure the focus is on delivering improved consumer outcomes:

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

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

- investing in and enabling AI and ADM innovation in the not-for-profit sector to demonstrably improve community outcomes and welfare
- implementing regulatory sandboxes to enable the safe testing and learning environment prior to deploying AI and ADM-enabled products and services at scale, and
- requiring businesses to meet specific public reporting obligations on how they use and test AI, the data sets they utilise, and outcomes (expected and actual).

Implementing a best-interests duty or duty of care obligations

The interests of Australians must be front of mind for businesses implementing any data-based initiatives, including the use of AI. The obligation to act in the interests of others is not new or even unique. For example, the financial sector requires that many professions act in the best interests of customers via fiduciary duties. In sectors such as disability, medical and aged care there is an obligation to act in the interests of others via common law duty of care.

CPRC consumer research confirms that Australians support their data being used with their best interests and the interests of the community in mind. Our national survey found that Australians believe:

- personal information should only be collected and used in a way that personally benefits them (70%)
- their personal information should not be collected and used in a way that harms them or others (83%), and
- personal information should only be collected or used if it is in a person's best interest and is unlikely to cause harm to them and others (70%).[22]

CPRC recommends that the Federal Government embed a best-interests or duty of care obligation as part of its approach to privacy protections which would then apply to AI-enabled systems as well.

Such an obligation would naturally shift the onus of responsibility from consumers to businesses. A best interests or duty of care obligation would:

- help move away from individual level of consent and shift the focus to system set-up and embedding safety by design

[21] AHRC, "Using artificial intelligence to make decisions", (November 2020), https://humanrights.gov.au/our-work/technology-and-human-rights/publications/addressing-algorithmic-bias-ensure-ethical-ai.

[22] *Ibid*

- protect people that may have the inability to consent such as children, people living with a disability or other consumers who are unable to participate in the consent model regardless of how well it may be set-up
- align interests of organisations and consumers as taking on new data will mean taking on new responsibilities and this can encourage a culture of data minimisation (collect only what you need not what you think you might need), and
- address issues of trust and confidence in both government and industry.[23]

A practical option is to consider a best-interests obligation that is broad but is supported by clear guidance and rules, including no-go zones which could evolve over time, with the regulator having the power to regularly review and update guidance and no-go zones instead of them being enshrined in legislation.[24] A similar example of this is the United Kingdom's Financial Conduct Authority's Consumer Duty which has a broad principle to act to deliver good outcomes but is supported with detailed guidance on what that looks like.[25]

Increasing regulatory understanding of AI and coordinating action

As outlined above, our strong preference is for a baseline of technology-neutral consumer protections that require businesses to treat customers fairly. Ultimately, all regulators will need to understand how AI is being used by the sectors they regulate and how industry-specific laws will apply. There is some risk that some regulators will have fewer resources or capability to engage with AI issues in their domains, and some AI issues will need to be addressed across multiple regulators. To address this, there is value in looking at how a Government-funded expert role or body could coordinate discussions and increase knowledge about AI across regulators and government bodies. This may look similar to, for example, the proposal raised by the Human Technology Institute for an AI Commissioner.

Question 14: Do you support a risk-based approach for addressing potential AI risks? If not, is there a better approach?

Question 15. What do you see as the main benefits or limitations of a risk-based approach? How can any limitations be overcome?

CPRC supports a risk-based approach for addressing potential AI risks combined with technology-neutral improvements to Australia's overall consumer protection framework, outlined above. We recommend that the Federal Government continue to observe the implementation of risk-based models that are proposed both in the UK and Canda. We agree that harmonising with international jurisdictions can help reduce regulatory burden but any alignment must be considered in how effectively it will mitigate harm for Australians.

There are two limitations that can be foreseen with a risk-based approach:

- If risk ratings are only identified at a point in time and cannot be adjusted or challenged by the regulator.
- If risk is left for businesses to self-identify.

As covered previously in our response to Question 5, regulators need to have the power to continuously review and probe systems for potential harm. As new possibilities of harms are identified, regulators should have the power to propose and/or adapt the level of risk given the highly dynamic nature of AI.

[23] CPRC, "In whose interest: Why businesses need to keep consumers safe and treat their data with care", (March 2023), www.cprc.org.au/inwhoseinterest.

[24] CPRC, "In whose interest: Why businesses need to keep consumers safe and treat their data with care", (March 2023), www.cprc.org.au/inwhoseinterest.

[25] Financial Conduct Authority (UK), "Finalised Guidance - FG22/5 Final non-Handbook Guidance for firms on the Consumer Duty", (July 2022), https://www.fca.org.uk/publication/finalised-guidance/fg22-5.pdf.

Identifying level of risk must be independent of the business, especially when there is high potential for consumer harm. While a business may initially nominate through self-assessment, there needs to be some form of regulatory oversight to confirm the accuracy of the assessment.

Question 20: Should a risk-based approach for responsible AI be a voluntary or self-regulation tool or be mandated through regulation? And should it apply to: a. public or private organisations or both? b. developers or deployers or both?

While AI may be an emerging frontier, the digital economy is not. We are beyond the waiting game now when it comes to developing adequate consumer protections for products and services in the digital economy. It is clearly evident that a self-regulatory or self-assessed approach is no longer adequate in addressing the risks posed to consumers by large and powerful businesses, some of which have predicated the success of their business models on creating information asymmetry and exploiting consumer vulnerabilities. Self-assessment is never impartial. **We can no longer expect businesses to act as both player and referee in the implementation of AI.**

We need the Federal Government to be proactive and not wait for Australians to endure harm first before creating safeguards for them.