Consumer Policy Research Centre

Level 6, 179 Queen Street, Melbourne, Victoria 3000

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

Submission to the Attorney-General – Privacy Act Review Report

30 March 2023

Submission made via: https://consultations.ag.gov.au/integrity/privacy-act-review-report/consultation/

Time for privacy reform that Australians deserve

It's time to introduce privacy laws that work to actively protect Australians in the digital economy.

Australians should no longer be expected to rely on notification and consent as a primary privacy protection measure. They should no longer have to accept unwieldy privacy policies which request consent to opaque data collection and sharing practices as a barter to access a product or service. They should no longer be subjected to having their data used in ways that takes advantage of who they are or what they're interested in for commercially beneficial outcomes.

The Consumer Policy Research Centre's (CPRC) latest research confirms that the status-quo is ineffective, inadequate, and incapable of delivering protections that Australians want and deserve:

- Only 7% of Australians feel that companies give them real choices to protect their privacy online.
- 84% agree that companies should act in the best interests of a consumer when using their data.
- Less than 10% are comfortable with the current approach to targeted advertising, where their behaviour can be tracked without consent.
- 50% don't know where to seek help if they have a problem with how a company is using or sharing data.

CPRC broadly supports many of the proposals outlined in the Privacy Act Review Report but recommends that the Federal Government strengthen protections further by:

- modernising what it means to be identifiable to cover information obtained from any source and by any means
- implementing 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
- requiring 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
- empowering the regulator to swiftly ban or restrict harmful practices that cause direct and clear consumer harms, and
- providing a clear pathway for redress when things go wrong.

Our submission uses insights from our research and addresses the proposals in the report using three key principles – fairness, safety and inclusivity for consumers engaging in the digital economy. Also attached are our two latest research pieces on privacy protections which look closely at the best interest concept and shows what consumers want from the Privacy Act review (Attachments 1 and 2).

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

Yours sincerely

Chandni Gupta
Digital Policy Director
Consumer Policy Research Centre

CPRC Summary of recommendations

Proposal	CPRC's position
Proposals 3.1 and 3.2 on the Objects of Act	CPRC supports these proposals.
Proposals 4.1 to 4.10 on personal information, de-identification and sensitive information	CPRC broadly supports these proposals but recommends two changes: Proposal 4.10, geotracking data should be recognised in the definition of sensitive data. Proposal 4.4 on 'reasonably identifiable', to effectively capture this obligation, CPRC supports the recommendation by Salinger Privacy to amend the definition of personal information within the Act and add, "*An individual is 'reasonably identifiable' if they are capable of being distinguished from all others, even if their identity is not known.*"[1]
Proposals 6.1 and 6.2 on small business exemption	CPRC supports the removal of the small business exemption, without exception. See *All businesses need to treat data with safety and respect* section below.
Proposals 10.1, 10.2 and 10.3 on privacy policies and collection notices	CPRC supports the proposals to ensure privacy policies and any notices on collection of personal information are clear and easy to understand, including through the use of standardised templates. CPRC recommends that any guidance developed on this is done so in consultation with a diverse set of consumer representatives and that government resource consumer user experience (UX) testing.
Proposals 11.1, 11.2, 11.3 and 11.4 on consent and privacy by default settings	CPRC broadly supports the proposals but the definition of consent should be strengthened. We support the Financial Rights Legal Centre (FRLC) proposal for the definition of consent to include the following amendments: • change unambigious to 'unambigious, indicated through clear action' • replace current with 'time-limited and specific', and • remove notion of implied consent or make a clear list of exceptions where implied consent may be legitimate. CPRC supports the development of guidance by OAIC but recommends that any guidance developed on this is done so in consultation with a diverse set of consumer representatives.

[1] See submission by Salinger Privacy: https://www.salingerprivacy.com.au/privacy-reforms/.

	CPRC also recommends that the government resource consumer user experience (UX) testing.
Proposals 12.1, 12.2 and 12.3 on fair and reasonable personal information handling	CPRC broadly supports the introduction of a 'fair and reasonable' test but recommends that consumer safety and care is embedded as part of the requirement. CPRC recommends that a best-interests or duty of care obligation be placed on all entities involved in the collection, sharing and use of consumer data. See *Implementing the 'fair and reasonable' test* section below.
Proposals 13.1 to 13.4 on Privacy Impact Assessment and other additional protections	CPRC supports the use of Privacy Impact Assessments. CPRC recommends that all businesses be obligated to conduct them.
Proposals 16.4 in regard to the best interests of the child	While CPRC supports Proposal 16.4, we recommend that the Attorney-General broaden this requirement so businesses are obligated to have regard to the best interests of **all individuals and the community** (not just children) as part of considering whether collection, use or disclosure is fair and reasonable.
Proposals 17.1, 17.2 and 17.3 on people experiencing vulnerability	CPRC broadly supports these proposals including the development of guidance by OAIC but recommends that any guidance developed on this is done so in consultation with a diverse set of consumer representatives in recognition that vulnerability is not always a static situation. CPRC recommends that safety and care obligations are embedded within the 'fair and reasonable test'. CPRC supports FRLC's recommendation that there be an obligation on businesses to implement the guidance and that the regulator monitors and audits entities to ensure guidance is being applied effectively.
Proposals 19.1, 19.2 and 19.3 on automated decision making	CPRC broadly supports these proposals. However, CPRC cautions that notification alone of the use of ADM technology which is then only included within a privacy policy is not adequate protection. While the proposals reference the use of broader regulatory work in AI ad ADM, the Federal Government must ensure this leads to fair, safe and inclusive outcomes for all Australians. CPRC supports Salinger Privacy's recommendation to "include a right to obtain a

	human review of a decision made by automated means".
Proposals 20.1 on introduction of definitions	CPRC supports the inclusion of clear definitions for direct marketing, targeting and trading.
Proposal 20.2 and 20.3 on unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes and receiving targeted advertising	**CPRC does not support this proposal. The default model should be for consumers to actively opt-in instead of opt-out.** This will give them genuine agency and control over their data. It also aligns with the privacy by default model quoted in the Privacy Act Report. For consumers who have opted-in, they then should have access to an unqualified right to opt-out. CPRC does not support any personal information to be collected for direct marketing without consent. See *Targeted advertising and direct marketing section* below.
Proposal 20.4 on obtaining consent to trade personal information	**CPRC does not support the trading of information, even with consent.** See *Trading personal information – people are not products* section below.
Proposal 20.5 on prohibiting direct marketing to a child unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests	CPRC supports prohibiting direct marketing to children. CPRC does not support the exceptions noted in proposal 20.5. The only exception would be for 'socially beneficial content' as noted in Proposal 20.8.
Proposal 20.6 on prohibiting targeting to a child, with an exception for targeting that is in the child's best interest	CPRC supports prohibiting targeting to a child. CPRC does not support examples referenced in the Report as being of 'best-interest'. The only exception would be for 'socially beneficial content' as noted in Proposal 20.8.
Proposal 20.7 on prohibiting trading in the personal information of children	CPRC support this proposal.
Proposal 20.8 on targeting to be fair and reasonable and targeted based on sensitive information be prohibited, with exception to socially beneficial content	CPRC supports this proposal but recommends, as previously stated, that safety and care obligations are embedded within the 'fair and reasonable test'.
Proposal 20.9 on requiring entities to provide clear information on use of algorithms and profiling to recommend content to individuals	CPRC supports this proposal.
Proposal 21.1 to 21.8 on security, retention and destruction	CPRC broadly supports the proposal. CPRC recommends that a key focus be given on how information is collected and stored to validate a person's identification which in a physical setting

	would only ever be sighted and not kept. This can be better managed with shorter retention periods or other mechanisms so personal information that is no longer needed is also no longer retained by entities. The Attorney-General must place clear obligations on businesses to reduce the risk of impact when data breaches occur. See *Dealing with data breaches* section below.
Proposals 25.1 to 25.11 on enforcement	**CPRC does not support this proposal as it does not create a strong enough approach to enforcement.** CPRC recommends that the Federal Government strengthen enforcement by allowing the regulator to proactively ban or restrict harmful data practices before widespread harm takes place. CPRC also recommends that the Federal Government consider establishing a Digital Ombudsman to support people to effectively access redress. See *Strong proactive enforcement and practical redress* section below.
Proposal 26.1 on a direct right of action	CPRC supports this proposal.
Proposal 27.1 on a statutory tort for serious invasions of privacy	CPRC supports this proposal.
Proposals 28.1 to 28.4 on notifiable data breaches scheme	CPRC recommends that when an entity is notifying individuals of a data breach relating to their personal information, the entity must also: • provide clear information on steps an individual may need to take, including where an individual can seek additional help and support • ensure there is a direct access for support and advice for individuals who are impacted, and • ensure any helpline or customer care line at the time of the breach is well-resourced for the influx of calls that an entity may receive. See *Data breaches* section below.

All businesses need to treat data with safety and respect

The size or nature of a business should not exclude it from ensuring that it treats people's personal information with safety, care, and respect. CPRC's consumer research confirmed that Australians expect the same level of privacy protections from small businesses as they do from businesses in general.[2] Australians agree that small businesses should:

- not collect information that they don't need for delivering a product or service (81% for small businesses, 79% for all companies)
- not collect information about them that they don't currently need for delivering the product or service (81% for small businesses, 84% for all companies)
- not share or sell personal information to another organisation without a person's explicit consent (82% for small businesses, 79% for companies to not sell information under any circumstances)
- take steps to keep their personal information safe (82% for small businesses, 84% for all companies).

When it comes to collection of information, the majority of Australians agree that small businesses should not collect personal information if they cannot ensure its safety and security (81%).

The results confirm that Australians expect that all businesses with which an individual shares their personal information with should be responsible for ensuring that the data is secure and is not shared or used in ways that may lead to harmful consumer outcomes.

CPRC supports the removal of the small business exemption, without exception. To ensure small businesses can meet the privacy obligations, CPRC supports the proposal for OAIC to provide guidance and support. Development of guidance and a support framework for small businesses should be high priority to ensure small businesses have the capacity and capability to comply with the requirements.

Implementing the 'fair and reasonable' test

CPRC broadly supports the Federal Government's proposal for a fair and reasonable test. However, the Government needs to ensure there is clarity that 'reasonable' will prioritise fairness and safety of those individuals whose data is being used and those who will be impacted by any decisions made based on the data.

The interests of Australians must be front of mind for businesses implementing any data-based initiatives. 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%)
- children's personal information should only be collected or used if it is in the best interest of the child and there is explicit consent from a parent or guardian (74%), 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%).[3]

CPRC recommends that the Federal Government embed a best-interests or duty of care obligation as part of its approach to privacy protections.

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

[2] CPRC, "Not a fair trade – Consumer views on how businesses use their data", (2023), https://cprc.org.au/not-a-fair-trade.
[3] *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.[4]

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.[5] 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.

There is already precedence of best interests of children being considered in the Privacy Act Report via Proposals 16.4 and 16.5. The opportunity is for the Federal Government to expand these proposals to apply to the best interests of all Australians, and not just a subset.

Targeted advertising, direct marketing and targeting

CPRC strongly recommends that the default model for targeted advertising and direct marketing should be for consumers to actively opt-in instead of opt-out to participate in these practices. An opt-in model will give consumers genuine agency and control over their data and aligns with the privacy by default model quoted in the Privacy Act Report.

CPRC's consumer research confirms that Australians have a clear discomfort with personal information being used for targeted advertising.[6] Less than 10% of Australians are comfortable with companies targeting them with advertising based on their online behaviour or personal characteristics even if they had not given permission. Close to half are not comfortable with companies targeting them based on their online behaviour (46%) or their personal characteristics (49%). Of those who are comfortable with targeted advertising, having the option to opt-out or having the option to opt-in are the preferred approaches.

Given that such a high percentage of Australians are uncomfortable with targeted advertising or would at least prefer that it is made available as an opt-in model, it is clear that an opt-in approach would be the safest option for Australians where the choice and control remain in their hands. Opt-in also should not mean that Australians are then subjected to dark patters / deceptive designs, including recurring notifications or nagging designed to coerce them into opting-in.[7]

Trading personal information – people are not products

CPRC does not support the proposal of trading of information, even with consent. CPRC's consumer research confirmed that Australians are uncomfortable with personal information being:

- collected from other companies (69% are uncomfortable)
- used to monitor their online behaviour (70% are uncomfortable)
- shared or sold with other companies (74% are uncomfortable).

Creating a consent process for trading personal information does not provide adequate protection from the harms that can take place through trading of personal information.

[4] CPRC, "In whose interest: Why businesses need to keep consumers safe and treat their data with care", (March 2023), www.cprc.org.au/inwhoseinterest.
[5] CPRC, "In whose interest: Why businesses need to keep consumers safe and treat their data with care", (March 2023), www.cprc.org.au/inwhoseinterest.
[6] CPRC, "Not a fair trade – Consumer views on how businesses use their data", (2023), https://cprc.org.au/not-a-fair-trade.
[7] CPRC, "Duped by design - Manipulative online design: Dark patterns in Australia", (2022), https://cprc.org.au/dupedbydesign/.

Dealing with data breaches

CPRC's consumer research confirmed that while majority of Australians agree that businesses should be responsible for keeping data safe (84%), there is little to no confidence in businesses actually doing this (less than 26%).[8]

Australians agree that businesses should:

- delete personal information when it is no longer needed (83%)
- protect them from harm if there is a data breach (65%)
- notify customers when there is a data breach and provide clear information about where to get help (86%).

CPRC recommends that any protections relating to data security and safety should ensure that businesses are held accountable to implement the above measures.

Strong proactive enforcement and practical redress

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.

To create an effective ecosystem for privacy protections, the Government must ensure the regulator is adequately resourced with the capacity and capability to monitor and enforce privacy breaches in this complex environment. It must be empowered to undertake proactive investigations.

CPRC consumer research confirmed that Australians expect governments to protect them against data misuse (88%). Australians also considered that the regulator 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)
- the power to ban data practices that cause harm (81% strongly agree or agree), and
- the ability to issue penalties for companies that breach privacy protections (82% strongly agree or agree).

CPRC proposes a Privacy Safety Regime that mirrors similar reforms that exist either in the Australian financial market such as the product intervention power[9] or the provision of bans under the Australian product safety framework.[10] Both reforms are designed to deeply reflect on emerging issues and ascertain how consumers may be protected from foreseeable harms.[11]

Why Australia needs to reimagine a new enforcement model for privacy

Traditional compliance and enforcement models often take place post harm. This needs to be reimagined if privacy protections are to be adequately delivered to consumers in the digital economy. Regulators need more sophisticated approaches to identify harm. Currently regulators largely rely on reports from consumers, identifying harm after it takes place. The majority of the onus cannot continue to remain on consumers and consumer groups to identify and report breaches. This is not sustainable in a digital environment where there are complexities in understanding how consumer data is collected, used, and passed on to other

[8] CPRC, "Not a fair trade – Consumer views on how businesses use their data", (2023), https://cprc.org.au/not-a-fair-trade.
[9] ASIC, "RG 272 Product intervention power", (June 2020), https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-272-product-intervention-power.
[10] 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.
[11] CPRC, "In whose interest: Why businesses need to keep consumers safe and treat their data with care", (March 2023), www.cprc.org.au/inwhoseinterest.

businesses. Instead, regulators need to proactively uncover harm that is currently obfuscated. Regulators should be pushing businesses to be radically more transparent about how they use consumer data.

Effective resourcing

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

Genuine redress for consumers

CPRC's consumer research confirmed that Australians are not confident in finding or accessing support mechanisms for when things go wrong online:

- 50% do not know where to seek help if they have a problem with how a company collects, shares or uses their personal information.
- 46% do not know where to seek help if their data is hacked.
- 46% 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.
- 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.

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, including privacy.

There must be effective dispute resolution pathways to enable consumers to seek redress for when things go wrong in the online space. As consumers increase their engagement online, a Digital Ombudsman needs to be adequately resourced to meet benchmarks for industry-based customer dispute resolution to ensure consumers can effectively resolve any disagreements that will arise.[12]

[12] See: Benchmarks for Industry-based Customer Dispute Resolution | Treasury.gov.au

Attachment 1

CPRC Report

Not a fair trade – Consumer views on how businesses use their data

CPRC WORKING PAPER

Consumer Policy Research Centre

Not a fair trade

Consumer views on how businesses use their data

cprc.org.au

Attachment 2

CPRC Report

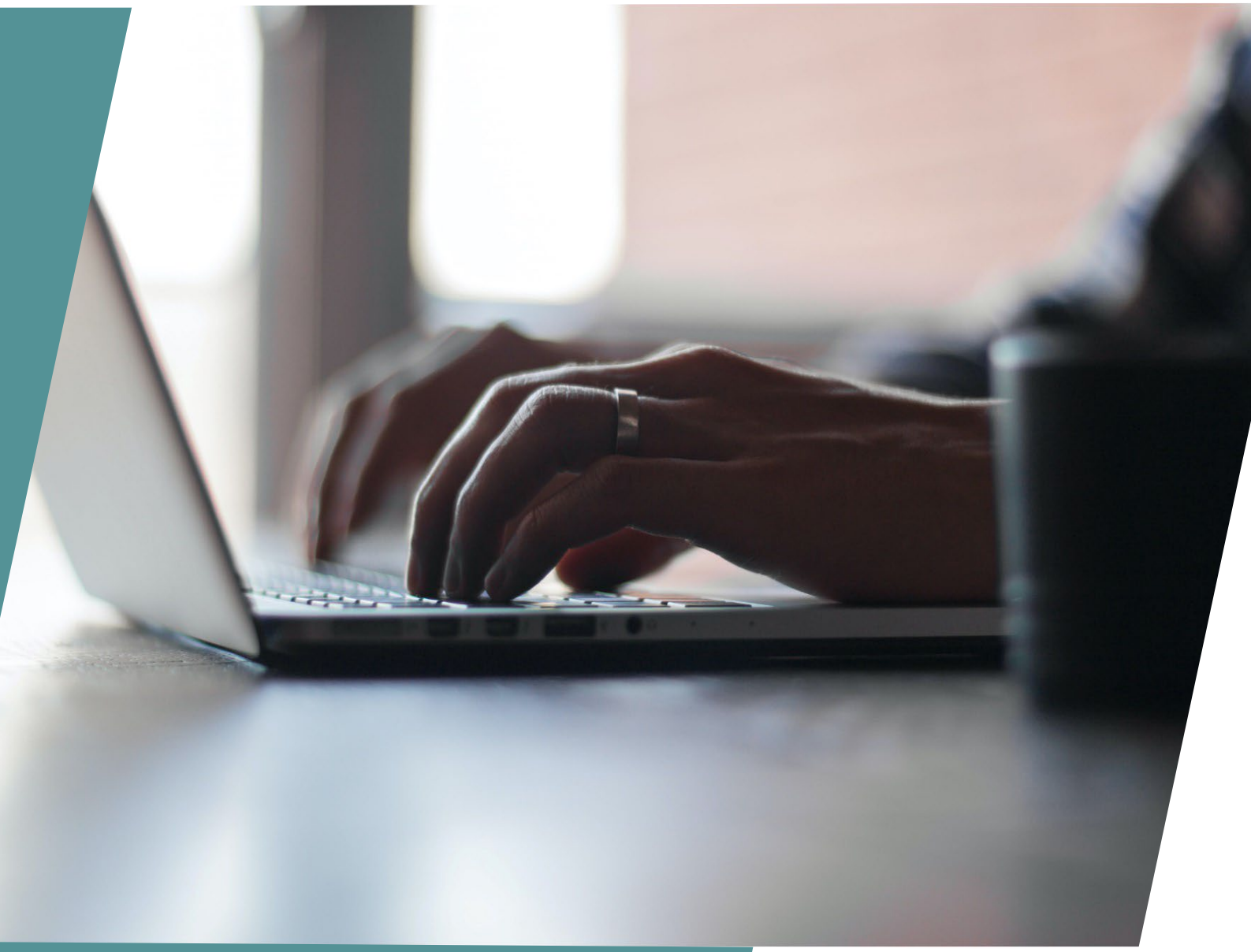
In whose interest – Why businesses need to keep consumers safe and treat their data with care

CPRC WORKING PAPER

Consumer Policy Research Centre

In whose interest?

Why businesses need to keep consumers safe and treat their data with care



cprc.org.au

CPRC

The Consumer Policy Research Centre (CPRC) is an independent, not-for-profit, consumer think-tank.
Our work is possible thanks to funding from the Victorian Government.

CPRC aims to create fairer, safer and inclusive markets by undertaking research and working with leading regulators, policymakers, businesses, academics and community advocates.

Acknowledgements

Report author: Chandni Gupta

CPRC would like to thank the following people and organisations for their input, time and advice:

- Dr Jeannie Paterson (UoM)
- Dr Katharine Kemp (UNSW)
- Dr Kayleen Manwaring (UNSW)
- Dr Ron Ben-David (CPRC Board Member)
- Australian Communications Consumer Action Network
- CHOICE
- Consumer Action Law Centre
- Digital Rights Watch
- Financial Rights Legal Centre
- Foundation of Alcohol and Research Education

The views expressed in this report should not be attributed to them. CPRC is responsible for the views in this report, including any errors or omissions.

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.

Published by Consumer Policy Research Centre

Suggested citation: Consumer Policy Research Centre, In whose interest: Why businesses need to keep consumers safe and treat their data with care, March 2023

cprc.org.au

Table of contents

Introduction – moving beyond notification and consent

Issues of safety and fairness can no longer be regulated using consumer choice as the primary protection. Instead, consumers need a privacy law that stops harmful business practices before they cause significant harm.

As Australia and the world propel forward with more data and digital innovation than ever before, the onus continues to be placed on consumers to "choose" – choose accordingly, choose carefully, choose thoughtfully. Choice is touted as the antidote for navigating the complex digital economy. Yet, we now know through a myriad of behavioural studies that the market economy and governments at large have overestimated the extent that consumers can make informed and rational decisions with little market intervention to stop harm, especially in a fast-paced digital economy.[1]

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 with a business but bear the consequences potentially for the remainder of their life is not a fair trade.

CPRC's previous research has confirmed that consumers consider the following common data practices to be unfair:

- Using personal information to make predictions about consumers.
- 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.

These are just the unfair data practices that the community is currently aware of. As data and digital innovation continue to grow in scope and velocity, new unfair practices and harms are likely to emerge. How do we create a digital experience that is fair, safe and inclusive to facilitate consumer trust in the growing digital economy? Many experts and organisations, including CPRC, have called for Australia's privacy law to go beyond consent. This paper looks deeply at what "beyond consent" options are available to protect consumers from harmful data practices.

Two concepts are explored in this working paper to address both current and emerging data harms:

- **Duty of care or best-interests duty**: operating similar to fiduciary duties in the finance sector to hold businesses accountable for how they collect, share, and use consumer data.
- **Privacy Safety Regime**: borrowing concepts from product intervention powers and product safety interventions, we propose options that would allow governments and regulators to stop or limit obviously harmful uses of data as well as a process for regulators to proactively restrict and test new harmful practices as they evolve.

The law needs to require more effort on the part of businesses to assess whether how they collect, share, and use data that results in fair outcomes for their customers. This burden can no longer remain on the shoulders of Australian consumers.

Methodology

The development of this paper has involved a combination of desktop and analytical research to identify how best-interest and duty of care obligations work across Australian and international legal frameworks. Research also involved analysis of different frameworks that are used to introduce temporary and permanent interventions when harm or the likelihood of harm is identified by regulators or governments.

This working paper benefited from advice and guidance from a variety of consumer and privacy experts, including academics (all are noted as experts when referenced in the working paper). CPRC collaborated with experts via one-to-one meetings and facilitated a roundtable held in December 2022. The roundtable also included a sketch artist from the Sketch Group agency who live illustrated the key discussion points. The imagery in this working paper is from those illustrations.

The aim of the discussions and the roundtable was to test the concepts outlined in an initial draft working paper. This published working paper takes into account the advice and guidance provided by the experts, for which CPRC is very grateful.

Duty of care or best-interests duty

Imagining businesses acting in the interests of consumers

Other laws that require businesses to act in consumer interests

The obligation to act in the interests of others is not new or even unique. 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. It is also a concept that is being explored by academics in the energy sector.[2]

Within the digital economy, this concept currently has been implemented through the New York Privacy Act's (NYPA) Data Fiduciary Obligation[3] and via a duty of care for large technology platforms in the European Union.[4] In the United Kingdom, the proposed Online Safety Bill proposes a statutory duty of care for social media companies to keep their users safe and tackle illegal and harmful content on their platforms.[5] The duty of care sits within UK's broader negligence law framework which requires businesses to a duty of care to *"…the general public who use the facilities they create and enable*".[6] However, this concept within consumer data is relatively new and unexplored in the Australian context.

A fiduciary duty traditionally is simply an expectation that an entity in a position of trust will act in good faith.

Within a traditional construct, a fiduciary duty is often set between individuals. The fiduciary is responsible for making decisions that are ethically and legally in the best interest of the trustee (often referred to as a client).[7] While a duty of care may be seen as a broader concept, in some jurisdictions, such as the United States, a duty of care is embedded within a fiduciary duty framework which also includes a duty of loyalty (i.e. there are to be no conflicts with the interests of the client).[8]

In other settings, such as superannuation, the fiduciary duty operates less in a binary model as it expects the fund to act in the collective interests of its members.[9]

The 2023 Privacy Act Review Report has already proposed a type of best-interest duty that is specific to children, noting that the law should "*require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances*".[10] The opportunity here is for the Federal Government to expand such a proposal to apply to the best interests of all Australians, and not just a subset.

Shifting the burden

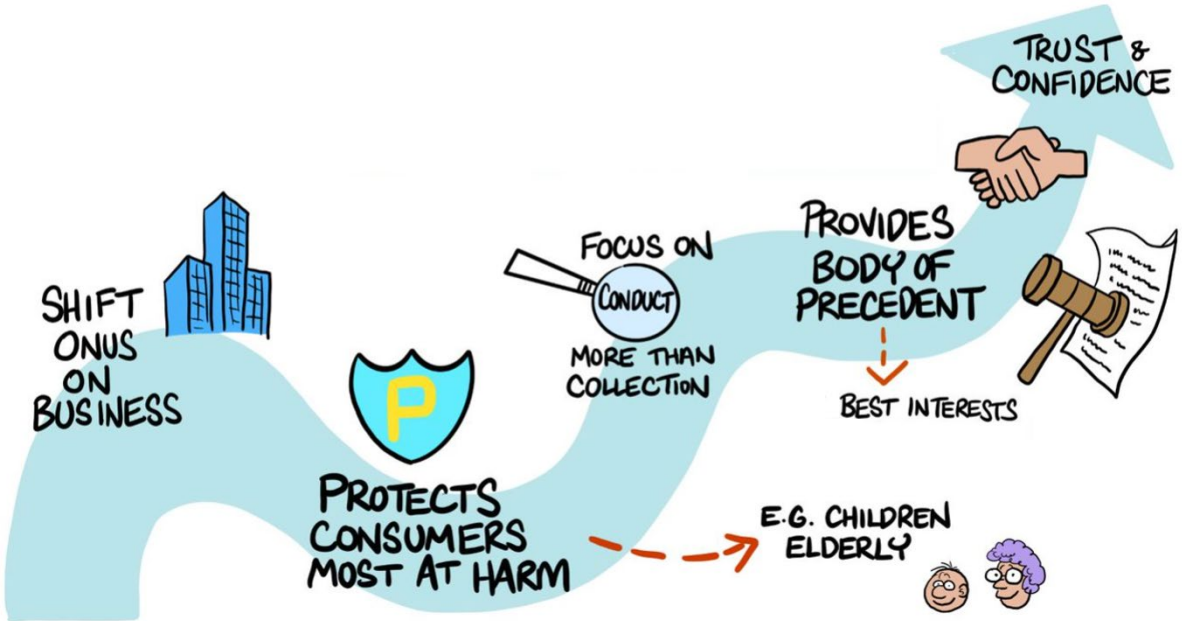
A best-interest or duty of care obligation shifts the onus onto businesses instead of holding consumers accountable to search for their best interests in a market economy that hasn't been developed with their interests in mind.

As an example, duty of care in an energy setting is being explored as imposing a "*positive responsibility on service providers… ensure compatibility between the provider's service offerings and customer's best interests*".[11]

When it comes to how consumer data is treated and how choice architecture (the way a website or app is designed to influence how and what people choose) is presented and implemented on digital platforms, a best-interests duty or a duty of care model has the potential to provide a strengthened consumer protection framework. These concepts can help add a level of accountability on digital platforms that could significantly reduce the likelihood of consumer harm. It could also lead to pro-business benefits by increasing consumer trust that businesses will look after them.

Feedback from many consumer and privacy experts confirmed that a broader duty of care or best-interests framework would naturally shift the onus of responsibility from consumers to businesses. Such an initiative could:

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



The tech neutrality of a broader framework that applies market-wide also makes it flexible to use across different technologies and tech industry. It moves away from the notion of regulating the consumer data aspect of specific technologies individually (e.g., artificial intelligence, facial recognition).

With the balance of responsibility tilting more towards the business in these models, an objection that can surface from industry is whether regulation in the data and privacy space will thwart innovation and limit the potential of the data at hand. However, the focus will need to shift to innovating for good, instead of innovating for the sake of profit. As Professor Jeannie Paterson of University of Melbourne noted in CPRC's webinar on unfair trading practices, "*Fairness doesn't stifle innovation, it just channels us to the right kind of innovation*".

What could a duty of care or best-interests duty look like?

A duty to individuals or to care for the collective?

While it appears to be a clearer and more familiar remit, in the data and privacy space, a one-to-one model may pose limitations to protections. It is now well-understood that individual data points and insights in aggregate can impact the products, services, and experiences of collective sets of individuals or communities. Also, given the significantly large number of users across many of the businesses that collect data, an effective system would need to expect a business to operate in good faith for large groups or the public as a whole.[12]

A broader framework that considers fairness and safety brings the opportunity to incorporate elements that may not have yet been considered in competition and consumer protection frameworks for digital settings.

A duty of care can be embedded within a fiduciary duty, but its focus is two-fold – avoiding practices that cause harm and putting in measures to ensure beneficiaries of the duty are protected from harms.[13]

For any new protection, Government must focus on limiting harms when businesses collect, share, and use consumer data. Often harm is obfuscated, and consumers are unable to assess the risk of current or future data harms, on themselves and on others.[14]

Even if consumers are given adequate information about how their data will be used, there still remains an asymmetry in power because, "*one party controls the design of applications and the other must operate within that design*".[15] CPRC's own research into dark patterns confirms that the prevalence of manipulative and deceptive design causes consumer harm. Australians have lost money, lost control of their data or have been manipulated by businesses to make choices that are not in their interests.[16]

Principle or prescriptive?

When considering a duty of care or a best-interests duty one element to explore is how it should be enshrined in law. Laws could be drafted to deliver:

- a general duty of care or best-interests statement that is broad to cover current, emerging, and future harms
- a prescriptive best-interests duty with specific bans and restrictions where the regulator is given authority to evolve the prohibitions over time, or
- a mixture of the two options with a flexibility for the regulator to impose new bans and restrictions.

How can businesses commit to fairness and safety?

A high-level principled approach could be enshrined into legislation. It could be as simple as the following statement:

> *A business must only collect, share, or use data in a manner that is in the consumer's best interest and avoids causing consumer harm*

The New York Privacy Act's data fiduciary obligation goes one step further by noting that it must be in the best interests of the state's citizens, "*regardless of how that impacts the interests of the business*". It captures the essence of fiduciary duties so when they come in conflict with the shareholders of a business, the duty to the consumer is given priority.[17]

In Europe, the Digital Services Act (DSA) calls for a duty of care but only for Very Large Online Platforms and Service Engines (VLOP and VLSE). While broad in its obligation, the DSA does outline the requirement of undertaking risk assessment, having a pathway to mitigate risks and conducting independent audits at their own expense.[18] There are mixed views on this duty of care, with some suggesting it as "ground-breaking" with its effectiveness becoming clearer with the introduction of specific legislation and guidelines,[19], while others claim that it is vague and lacks legal certainty.[20]

The above proposed statement could be also expressed inversely by outlining that a business cannot collect, share, or use data that is not in the consumers' best interests. This may limit the scope of what's expected but a broader duty can raise enforcement challenges. A broader framework could impose a positive duty on a business's data-based practices so they are implemented having both the individual's and the community's best interests in mind.

Whose data is it anyway?

Developing such a duty will require exploration of how to construct such a principle within regulatory measures relating to privacy. One particular issue to explore is how ownership of data is defined. Currently, there is a sense that the businesses who collect consumer data are in fact owners of that data. However, if data points (including direct and those related to) are all considered personal information, which they should be, then ownership and therefore duty of care can be effectively developed with the consumer being at the heart of that care.

One option is to consider if data could be defined as it is currently in the Consumer Data Right[21] (CDR) framework. Within CDR, there are clear parameters between data ownership and data access. It is understood that consumers are data owners and businesses who collect consumer data are data holders and other intermediaries that may have access to the data are accredited data recipients. Such a model, if implemented thoughtfully, can further shift the focus towards 'doing right by the consumer'.

One factor that the CDR framework does not address is the ownership of insights gained from collection of data. By default, it can be implied that in the current ecosystem, insights belong to the business. Within a best-interests or duty of care model, some aspects relating to insights could be dealt via the responsibilities linked with the use of data. A duty could expect that insights curated from data points, in particular those that lead to decisions on products and services offered should not leave consumers worse off.

The insights gained should be used to create a more positive and safe experience that is more meaningful for consumers. Currently, some of the harms that can take place due to ill-informed insights often originate from the lack of human oversight over algorithmic decision-making, often set up to identify and act on insights.[22] That lack of oversight can make it difficult to assess whether insights from specific data points accurately pinpoint a causation or whether it is simply coincidental correlation.[23] In the report by Human Technology Institute on facial recognition, the authors highlight a range of issues that could also be applied to use of data settings. Two in particular are the problems noted as “system error” or “abuse”. System error is where the facial-recognition technology (FRT) accurately identifies an individual but aggregates other data incorrectly to produce inaccurate and potentially harmful decisions. Abuse relates to “deliberate misuse” of the FRT such as racial profiling.[24] These concepts could be embedded into a data duty to help create limitations on how insights are curated and utilised.

Practical options to make a duty a reality

Clear no-go zones

CPRC's previous research into exploring an unfair trading prohibition considered 'blacklists' as an approach to provide a clear expectation on what businesses can and cannot do. The same could be imagined within a duty of care setting. A more prescriptive form of accountability may make enforcement more clearcut, but rogue businesses are also likely to find loopholes that sit outside the 'no-go zones' that may still not be in the best-interests of the consumer.

Blacklists are used in legislation such as the Unfair Commercial Practices Directive in Europe and Consumer Protection (Fair Trading) Act in Singapore, both of which include adjunct documentation outlining specific business practices that are deemed unfair under their laws.[25]

Blacklists of harmful practices can be applied to specific types of data such as de-identified data which may need to be defined given that a broad framework may still be limited in its scope for such form of data. One example that was shared included a gambling platform purchasing de-identified data from a bank. A blacklist could ensure that such practices could be identified as a clear no-go zone enshrined into law under a broader framework. De-identified data may not necessarily impact an individual, but its aggregation and use may impact a group or community.[26] Experts highlighted that de-identified data can still be rich and valuable with the potential to be used against others that might fit a similar description but aren't part of the original data set.

High-level principle with evolving guidance

It is likely that a more practical option is a framework that is broad but is supported by clear guidance and rules on data practices, including 'no-go zones' that evolves over time, noting that enforcement would not be limited to just these. Also, to ensure rules and the 'no-go zones' are fit for purpose in the current and emerging data-enabled environment, ideally it would be a measure that the regulator could have power to regularly review and update, instead of being enshrined in legislation.

An example of a broad approach to a duty of care that is supported via specific rules is the Financial Conduct Authority's (FCA) Consumer Duty in the United Kingdom which will come into effect from July 2023 onwards. This principles-based Consumer Duty requires businesses to "*act to deliver good outcomes for retail customers*".[27] The broad Consumer Duty is split across three key requirements.

> *"The cross-cutting rules require firms to:*
> - *act in good faith*
> - *avoid causing foreseeable harm*
> - *enable and support retail customers to pursue their financial objectives."*[28]

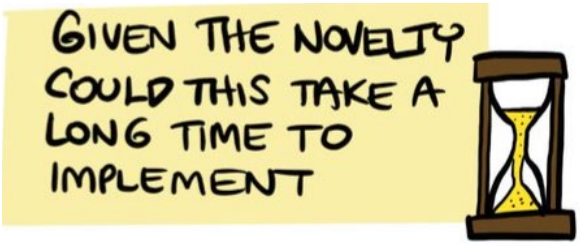
The guidance supporting the Consumer Duty and each of its three requirements outline conduct that businesses should and should not be engaging in. As an example, under the requirement 'Avoid causing foreseeable harm', there is a specific list of examples of foreseeable harms which includes conduct relating to the inability to cancel a product or service or incurring high fees due to lack of appropriately tailored information disclosures.[29]

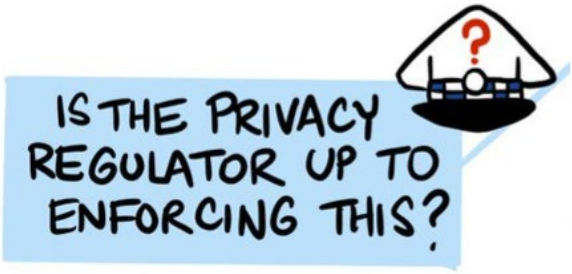
Such a model can provide the regulator with a broader remit if the regulator is adequately resourced to undertake more proactive enforcement. While we are yet to see the implementation of FCA's Consumer Duty, it is a model that has potential to be replicated in a data and privacy setting.

Embedding a fair and safe framework in law

There is, as in any broad framework, the possibility that a best-interests or duty of care obligation will create regulatory loopholes, especially in identifying which entities a broad duty applies to when the data supply chain is not a linear one-to-one process. A duty may be difficult to enforce given it also requires different enforcement skills and a different regulatory culture – one that is proactive, well-resourced and can identify and enforce issues before widespread harm occurs. Two options were explored by experts:

1. Framing the duty as an obligation.
2. Implementing a tiered approach to best-interests.

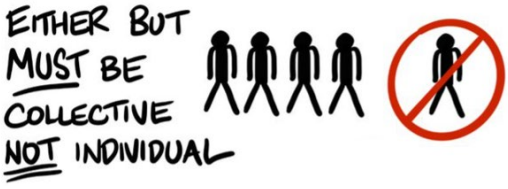




Framing the duty as an obligation

One option is to frame the duty as an obligation to not harm those who will be impacted by the decisions based on the data used. This would also help broaden the scope to the analysis of de-identified data which was raised earlier in this paper. This would be a collective approach which experts noted would likely be a better way to proceed but could face arguments within a law and economics space.

A collective duty could be seen by some as vague, and rogue organisations may take advantage of this to undermine a duty to the individual. Experts also noted that a collective "interests" duty is less commonly used in legislation. Most interest duties



place obligations on individuals to protect individuals (e.g., financial advisers and their clients or doctors and their patients).

There are limited examples of broad duties (e.g., in superannuation). To counter this, another option would be to place a positive obligation on businesses to 'do good' and use data to create opportunities for a better world.

Tiered approach to introducing fairness and safety as a business obligation

One approach could be to consider leading with implementation of specific best-interest or duty of care obligations to help reform how businesses think about how and what data they are collecting rather than litigating after a harm as occurred.

A tiered approach may help Government to change business conduct over time, first starting with a shift in mindset. This could be implemented in many ways:

- Limit the initial application of a best-interest framework or duty of care obligations towards their customers (i.e., individuals not businesses who may also be their customers) followed by introducing a broader framework of fairness and safety that embeds a collective duty.
- Limit the initial application to larger platforms, similar to how the duty in the Digital Services Act in the EU will only apply to Very Large Online Platforms (VLOP) and then broaden the scope to more businesses over time with support to implement the new mindset.
- Expand the current Australian Privacy Principles (APPs) to include best interest – with a clear indication of how this duty interacts with directors' duties.
- Incorporate best interest duty as part of a tort.
- Develop clear 'Guidance' or examples which are binding (i.e., when new conduct is identified, there needs to be a clear and effective way to add to an evolving blacklist). Any guidance, including a blacklist with examples will need to be carefully drafted to ensure best interests can still be broadly interpreted and enforced by the regulator.

One limitation with a tiered approach is the disparity it can create in the market. Creating a tiered approach or excluding specific types of businesses can continue to create loopholes for poor online practices to thrive. It also places the onus on consumers to navigate a complex market to determine which businesses are obligated to act in their best interest and which ones do not. This adds further burden on consumers who already feel overwhelmed when it comes to engaging online.[30]

A way to mitigate this issue, is to outline a detailed timeframe and process to how a tiered approach would be implemented, building in expectations upfront that the ultimate goal is for the entire market to eventually comply with the obligations. This form of a tiered approach is not new and can help a market to progressively reach a desired outcome for consumers. As an example, in 2019, the new mandatory product safety standard for quad bikes was introduced in two stages where the initial stage involved meeting specific standards, testing and labelling requirements. The second stage (effective one year later) then introduced obligations for protection devices and minimum stability requirements.[31] The transition to the mandatory standard was supported by various guidance for both dealers and manufacturers.[32]

Privacy safety regime

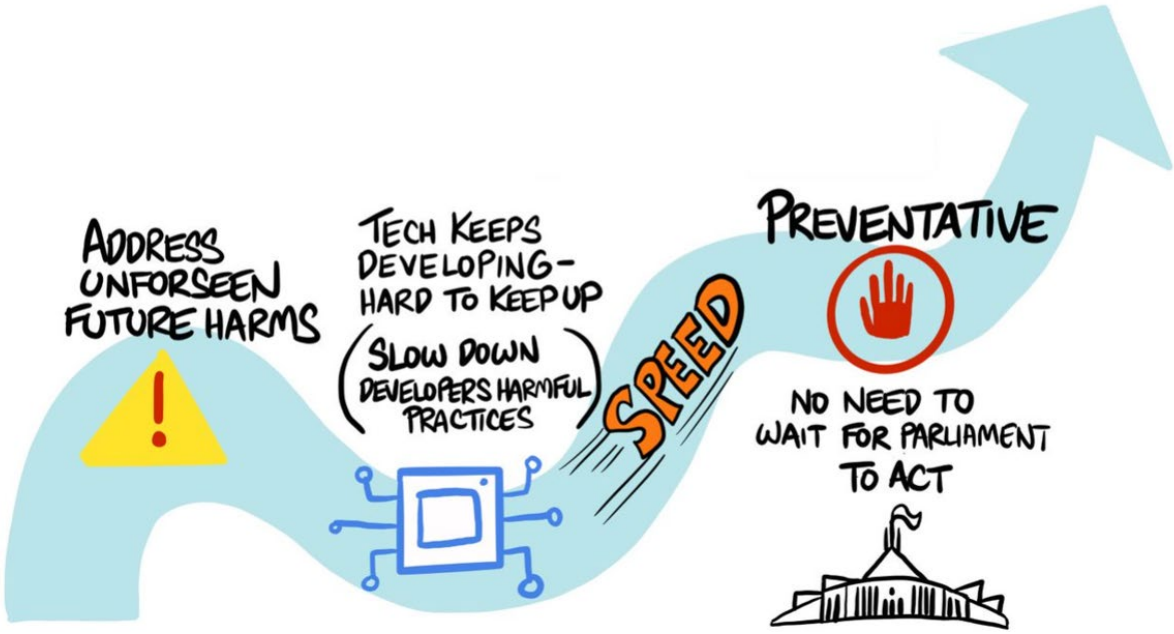
Safety at the heart of privacy

The privacy regulator needs new powers to keep consumers safe

We need our regulators to stop obviously harmful behaviour and practices before widespread harm occurs and to have the power to restrict likely harmful practices while investigations take place.

One way to achieve this could be via a concept CPRC has termed as a Privacy Safety Regime. Such a regime could mirror similar reforms introduced in the Australian financial markets such as the product intervention power and consider measures currently in Australia's product safety framework that are used to investigate emerging product safety hazards. Feedback from experts confirmed that a proactive approach to pause and assess data practices could effectively deal with new and emerging technologies and help drive positive change in business conduct to make safety a priority.

CPRC's research thus far has confirmed that Australian consumers strongly support further privacy protections. CPRC's 2020 research found that 74% of Australian consumers have safety concerns in relation to being targeted with particular products or services, 76% consider it to be unfair when their personal information is used to make predictions about them and 80% consider it is unfair for their personal information to impact what products they are eligible for.[33]



How do other regulators stop emerging harms?

Product intervention power

In 2018, the Federal Government introduced product intervention powers under the Australian Securities and Investment Commission's (ASIC) remit. This means that ASIC can place a temporary prohibition on a financial or credit product. It has enabled ASIC to make product intervention orders on financial products that are causing or at risk of causing consumer harm.[34]

As an example, in 2022, ASIC placed a product intervention order on short term credit and continuing credit contracts involving high fees to consumers for small amounts of credit.[35] This was an intervention that ASIC could implement independently to the Federal Government, meaning it could be brought into application within the market far sooner than it would have had it gone through the usual route of legislative review and change.

Unlike traditional enforcement where issues are investigated after harm has taken place, a product intervention power has meant ASIC can take a more proactive approach to market regulation. In its guidance documentation, ASIC notes the following powers that it now has as a regulator via the product intervention power:

> *"The power:*
>
> *(a) enables us to respond to problems in a flexible, targeted, effective and timely way*
>
> *(b) enables us to take action on a market-wide basis, and*
>
> *(c) is available without a demonstrated or suspected breach of the law, which enables us to take action before significant detriment, or further detriment, is done to consumers, so that we can better uphold community expectations on the conduct of firms that issue or distribute products".*[36]

A similar product intervention power also exists in the United Kingdom. The FCA has authority to make rules in the interest of "*consumer protection, competition and market integrity*".[37] Rules generally require public consultation before being introduced but in specific circumstances the FCA has power to make temporary product intervention rules (valid for up to 12 months) before undertaking consultation. FCA notes the following circumstances when a temporary product intervention rule can be made.

> *"Some of the instances in which the FCA might consider making temporary rules include:*
>
> - *where a product is in serious danger of being sold to the wrong customers, for instance where complex or niche products are sold to the mass market*
> - *where a non-essential feature of a product seems to be causing serious problems for consumers, and*
> - *where a product is inherently flawed".*[38]

In contrast, ASIC does not have the flexibility to impose product intervention orders of any kind without first undergoing public consultation.[39] While there may be perceived market risks when FCA introduces a temporary product intervention order without consultation, it does mean that a review of a product or service can be fast-tracked to limit consumer harm. It effectively pauses the conduct while the regulator conducts rigorous investigation and consultation ensuring that no further consumer harm takes place.

Interim and permanent product safety bans

Within the Australian Consumer Law under the *Competition and Consumer Act 2010*, the Commonwealth Minister and the respective state and territory fair trade or consumer protection Ministers can enforce an interim ban for products that have or are likely to cause injury.[40]

Unlike introducing a mandatory standard, which can involve a lengthy regulatory process, an interim ban can be imposed and be effective immediately for up to 60 days and extended to a further 60 days, if needed. Within this time period, the Australian Competition and Consumer Commission (ACCC) will assess the risk of consumer harm and, if required, it may recommend to the Commonwealth Minister to impose a permanent ban.[41] For example, in 2009, the Commonwealth Minister initially imposed an interim ban on sky lanterns due to these products posing a fire risk. Following the interim ban, the Commonwealth Minister issued a permanent ban on these products.

Sky lanterns, also known as flying paper lanterns, resemble miniature hot air balloons that lift into the atmosphere with the support of an open flame inside the lantern.[42] While no injuries or near-miss incidents had been reported in Australia, the imminent risk of fire due to Australia's drought-prone environment, was adequate to impose the ban.[43] Unlike a mandatory standard which involves significant evidence of harm either in Australia or overseas along with a detailed Regulatory Impact Statement, an interim ban can help bring safeguards to consumers immediately and help fast-track an assessment process towards more long-term measures.

One particular shortcoming of this framework that was explored by experts was its reliance on Ministerial intervention, even to introduce temporary restrictions. This can increase the likelihood of delay and can potentially politicise what would otherwise be an issue of consumer safety. If the Federal Government was to consider such a model for privacy, the regulator should have the independency to at least introduce an interim ban so measures to protect consumers can be implemented swiftly.

Considerations for a privacy safety regime in Australia

One of the key benefits of both the product intervention powers and product safety interim bans is their timeliness to deal with emerging and potential consumer harm. It also enables the regulators and Government to impose a pause on a practice or product while they proactively assess the risk. This ability to proactively intervene to stop emerging harm is currently missing from Australia's privacy regulations.

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.[44] Instead, we are relying on the good faith of businesses to stop using this controversial technology, many of which are placing commercial benefits of data harvesting over the safety and wellbeing of Australians.

Effective resourcing

Adequate resourcing or lack thereof can impact how an intervention, or a ban is developed and enforced. Experts noted that either framework can be resource intensive for regulators. Regulation costs can be high requiring the regulator to have both the capacity and capability at any given point in time when an issue is raised. Building evidence of harm may also prove difficult as there is a risk of capturing positive uses cases. Interventions or bans need to be broad enough to apply market-wide but focused enough to restrict the specific practices that are causing or likely to cause harm.

One possibility explored with experts to mitigate the resource constraint likely to be faced by a regulator, is for the Federal Government to consider an industry payment model by introducing levy penalties based on how much data is held by a business. This could encourage data minimisation as much of the harm is often derived from hoarding and transferring data. Another option would be to resource consumer organisations to assess and raise issues in a format similar to a super-complaint.[45]

Conclusion

Australia is at the cusp of delivering privacy protections that Australians need and deserve. Considering privacy protections as an opportunity to provide both care and safety to consumers enables Australia to foster a digital economy where consumers can thrive. It can become a digital economy that supports instead of manipulates consumer choice, builds trust instead of embedding opaqueness.

The ideas outlined in this paper show that safety and care are standards that consumers need businesses to meet and that could be practically developed as legal obligations.

Endnotes

[1] Nadler, A. and McGuigan, L., "An impulse to exploit: the behavioral turn in data-driven marketing", (2018), Critical Studies in Media Communication, 35:2, 151-165, https://doi.org/10.1080/15295036.2017.1387279

[2] Ben-David, R., "Energy consumers deserve a best interest duty", (June 2022), https://www.linkedin.com/pulse/energy-consumers-deserve-best-interest-duty-ron-ben-david.

[3] Romano Law, "Ready or Not New York, Privacy Here We Come: The Impending New York Privacy Act", (April 2021), https://www.romanolaw.com/2021/04/30/ready-or-not-new-york-privacy-here-we-come-the-impending-new-york-privacy-act.

[4] European Union, "Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)", (Accessed 5 November 2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014#d1e2731-1-1.

[5] UK Parliament, "Parliamentary Bills – Online Safety Bill", (Accessed: 2 March 2023), https://bills.parliament.uk/bills/3137 .

[6] Gelber, K., "A better way to regulate online hate speech: require social media companies to bear a duty of care to users", (14 July 2021), The Conversation, https://theconversation.com/a-better-way-to-regulate-online-hate-speech-require-social-media-companies-to-bear-a-duty-of-care-to-users-163808.

[7] Corporate Finance Institute, "Fiduciary Duty", (October 2022), https://corporatefinanceinstitute.com/resources/wealth-management/fiduciary-duty/.

[8] Tretina, K., "How Fiduciary Duty Impacts Financial Advisors", (15 July 2022), Forbes Advisor, https://www.forbes.com/advisor/investing/financial-advisor/what-is-fiduciary-duty.

[9] Cormican, L., "Super funds' fiduciary duty to participate in class actions", (July 2022), Super Review, https://superreview.moneymanagement.com.au/news/superannuation/super-funds-fiduciary-duty-participate-class-actions.

[10] Attorney-General's Department, "Privacy Act Review Report", (16 February 2023), https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report.

[11] Ben-David, R., "Minimising consumer harm for a successful energy transition", (November 2022), https://www.linkedin.com/posts/ron-ben-david-753a7940_minimising-consumer-harm-in-the-energy-transition-ugcPost-6999951284657102849-JxAl/.

[12] Balkin, J.M., "The fiduciary model of privacy", (2020), Harvard Law Review Forum, 134:1, https://doi.org/10.1080/15295036.2017.1387279.

[13] Arora, C., "Digital health fiduciaries: protecting user privacy when sharing health data", (2019), 21, 181-196, https://link.springer.com/article/10.1007/s10676-019-09499-x.

[14] Balkin, J.M., "The fiduciary model of privacy", (2020), Harvard Law Review Forum, 134:1, https://doi.org/10.1080/15295036.2017.1387279.

[15] *Ibid.*

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

[17] Véliz, C., "The ethical case for data fiduciaries", (November 2020), Ada Lovelace Institute, https://www.adalovelaceinstitute.org/blog/ethical-case-for-data-fiduciaries/.

[18] European Union, "Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)", (Accessed 5 November 2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014#d1e2731-1-1.

[19] Pirkova, E., "The Digital Services Act: your guide to the EU's new content moderation rules", (July 2022), Access Now, https://www.accessnow.org/digital-services-act-eu-content-moderation-rules-guide/.

[20] Article 19, "EU: Due diligence obligations in the proposed Digital Services Act", (May 2021), https://www.article19.org/resources/eu-due-diligence-obligations-in-the-proposed-digital-services-act.

[21] Consumer Data Right, "What is CDR?" (Accessed 1 April 2022), https://www.cdr.gov.au/what-is-cdr.

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

[23] Broad, E., "Made by Humans", (2018), Melbourne University Press, Melbourne Australia.

[24] Davis, N., Perry, L. & Santow, E., "Facial Recognition Technology: Towards a model law", (2022), Human Technology Institute, The University of Technology Sydney, https://www.uts.edu.au/human-technology-institute/explore-our-work/facial-recognition-technology-towards-model-law.

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

[26] Kemp, K., "Concealed data practices and competition law: why privacy matters", (5 November 2020), European Competition Journal, Volume 16, 2020 – Issue 2-3, https://doi.org/10.1080/17441056.2020.1839228.

[27] Financial Conduct Authority (UK), "A new Consumer Duty – Feedback to CP21/36 and final rules", (July 2022), https://www.fca.org.uk/publication/policy/ps22-9.pdf.

[28] *Ibid.*

[29] 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.

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

[31] ACCC, "Quad bikes", (Accessed 28 February 2023), Product Safety Australia, https://www.productsafety.gov.au/product-safety-laws/safety-standards-bans/mandatory-standards/quad-bikes.

[32] ACCC, "Quad bikes", (Accessed 28 February 2023), Product Safety Australia, https://www.productsafety.gov.au/products/transport/quad-bikes#toc-related-publications.

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

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

[35] ASIC, "19-250MR ASIC makes product intervention order banning short term lending model to protect consumers from predatory lending", (12 September 2019), https://asic.gov.au/about-asic/news-centre/find-a-media-release/2019-releases/19-250mr-asic-makes-product-intervention-order-banning-short-term-lending-model-to-protect-consumers-from-predatory-lending.

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

[37] Mathieson, M. and McLennan, M. "What do the product intervention powers of the UK financial conduct regulator look like?", (September 2014), Allens, https://www.allens.com.au/insights-news/insights/2014/09/unravelled-what-do-the-product-intervention-powers-of-the-uk.

[38] Financial Conduct Authority (UK), "FSA confirms approach to using temporary product intervention rules that will be used by the FCA", (25 March 2013), https://www.fca.org.uk/news/press-releases/fsa-confirms-approach-using-temporary-product-intervention-rules-will-be-used.

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

[40] 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.

[41] *Ibid.*

[42] ACCC, "Product bans – Sky lanterns" (Accessed 10 November 2022), Product Safety Australia website, https://www.productsafety.gov.au/product-safety-laws/safety-standards-bans/product-bans/sky-lanterns.

[43] Australian Government, "Explanatory Statement – Consumer Protection Notice No. 17 of 2011 – Permanent ban on sky lanterns" (Accessed 10 November 2022), https://www.legislation.gov.au/Details/F2011L00227/Explanatory%20Statement/Text.

[44] Pereira, A., "Complaint to OAIC on use of facial recognition in retail stores", (June 2022), CHOICE, https://www.choice.com.au/consumer-advocacy/policy-submissions/2022/june/complaint-oaic-on-use-of-facial-recognition.

[45] Office of Fair Trading (United Kingdom), "Super-complaints – Guidance for designated consumer bodies", (July 2003), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/284441/oft514.pdf.

CPRC

The Consumer Policy Research Centre (CPRC) is an independent, not-for-profit, consumer think-tank.
Our work is possible thanks to funding from the Victorian Government.

CPRC aims to create fairer, safer and inclusive markets by undertaking research and working with leading regulators, policymakers, businesses, academics and community advocates.

Acknowledgements

Report author: Chandni Gupta

CPRC would like to thank Dr Katharine Kemp of the University of New South Wales from our expert panel for her input, time and advice during survey development.

CPRC is responsible for the views in this report, including any errors or omissions.

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.

Published by Consumer Policy Research Centre

Suggested citation: Consumer Policy Research Centre, Not a fair trade: Consumer views on how businesses use their data March 2023

cprc.org.au

Table of contents

Introduction

The status quo where businesses collect, share and use personal information with very few restrictions or limits is not working for Australians.

The Consumer Policy Research Centre (CPRC) undertook this research to make sure that consumer views and needs were well-reflected in ongoing discussions about reform to Australia's privacy protections. Australian consumers told us very clearly what they want: for businesses to treat their data with greater care and respect.

Today, most protections for consumers are based on notification and consent. Practically, this means that people are asked to accept long and unhelpful privacy policies, often as the precursor to accessing a product or service. It's difficult, if not impossible, to really understand how a business will actually use your data. If you don't like what a business plans to do with your data, you typically have two choices: accept it or don't shop with that business. The take-it-or-leave-it approach to privacy policies doesn't give people real choice and doesn't offer meaningful protection against harmful data practices.

There's a major mismatch with how the digital economy currently works and what consumers want. Whole industries currently exist to trade in consumer data yet 79% of Australians agree that a company should not sell people's data under any circumstances. Even though companies commonly monitor what we do online, on their own websites as well as across the internet, 70% of people are not comfortable with companies monitoring their online behaviour.

Australians want all businesses to meet minimum standards for data collection and use. From a consumer perspective, the harm to them from poor data practices is the same whether it's caused by a small, large, local or international business – 90% expect businesses to protect against data misuse that leaves them worse-off.

These requests from consumers are reasonable. It is only in the past decade that many companies have come to expect that they can collect significant data about their current and potential customers, track them and on sell that data. With 79% of Australians agreeing that a company should only collect information that it needs to provide the product or service and 84% agreeing that data should be used with their interests in mind, it's time to shift the onus.

It's time for businesses to look at data and see how they can profit through positive outcomes for the community instead of monetising data in ways that cause community harm.

The law needs to require more effort on the part of businesses to assess if how they collect, share, and use data results in fair outcomes for their customers. Australians support a strong regulator that has sufficient resources to investigate privacy harms (82%) and has the power to pause, test and ban current and potentially harmful data practices (80% or more).

Australians deserve privacy laws that protect them, a regulator that has the power and resources to proactively enforce the law and a system that gives them access to support for when things go wrong. The burden for creating a safe online world and protecting privacy can no longer remain on the shoulders of Australian consumers.

Methodology

This report outlines key findings from a nationally representative survey of 1,000 Australians, exploring consumer views on how businesses collect, share and use consumers' personal information. It builds on some of the consumer research conducted by the Consumer Policy Research Centre in 2018 and 2020.[1] However, this survey was designed in a way to specifically capture consumer sentiment on issues related to proposals within the 2023 Privacy Act Review report.[2]

CPRC's survey was conducted between 10 and 16 March 2023. Data collection was conducted by CPRC, using Ipsos' Digital Platform. To achieve a nationally represented sample, quotas were set on each of the three demographic variables of age group, gender, state/territory.

The report also includes commentary from survey participants. Participants were invited to provide commentary at the end of the survey. As participants are completely deidentified, quotes in the report are attributed as "*consumer survey participant*".

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

[2] Attorney-General, "Privacy Act Review Report", (2023), https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

Key findings

Business accountability

Only **7%** feel companies give them real choices to protect their privacy online

84%
agree that a company should be responsible for keeping data safe

Only **15%** feel businesses are doing enough to protect their privacy

84%
agree that companies should always act in the best interest of the consumer when it uses their data

79%
agree companies should only collect information about them that they need to provide a product or service

Targeted advertising

Less than **10%** are comfortable with the current approach to targeted advertising with tracking of online behaviour or personal characteristics without giving expressed permission

70%
are not comfortable with companies monitoring their online behaviour

Sharing and selling consumer data

74%
are not comfortable with companies sharing or selling their personal information with other companies

79%
agree that a company should not sell people's data under any circumstances

64%
find it unfair that companies require you to supply more personal information than is necessary to deliver the product or service

90%
expect businesses to protect people's information from being used in ways that leaves them worse-off

Help and redress

52% agree that it's time-consuming to find actions to protect their privacy online

50% do not know where to seek help from if they have a problem with how a company collects, shares and uses their personal information

82%
agree that a regulator should have enough staff and resources to investigate how companies collect, share and use personal information

Defining what's personal

There is some confusion about what "personal information" is currently protected by the Privacy Act.[3] The Review of the Privacy Act puts forward a recommendation to clarify that "personal information" is meant to be a broad concept which includes information that could reasonably identify someone. This aligns with consumer views of what they think is personal information.

The survey asked Australians to select data points which they considered as personal information in addition to name, address, gender, telephone and date of birth (Figure 1). The top 10 categories considered as personal information were:

1. financial information (72%)
2. phone contacts (70%)
3. income (68%)
4. photos (64%)
5. messages (62%)
6. location data (61%)
7. IP address (60%)
8. device IDs (59%
9. mental health information (57%)
10. online search history (56%)

These categories were followed closely by physical health (56%), sexuality (53%), family members and ancestry (52%) and whether a person is living with a disability (50%).

While results are mixed to the extent of which data points are considered as personal information, only 3% of Australians considered none of the additional categories as personal information. Also, of all the suggested categories, the lowest ranking category (topics you are interested in) still had a significant portion of the population considering it as personal information (24%). This points to a recognition that Australians generally consider a lot more of their data points as personal information and any new consumer protections should ensure this information is adequately protected and, if used by businesses, that it is done so with safety and respect.

"Need to be more protective with personal information"

"Too much detailed information is being collected"

Comments from consumer survey participants

---

[3] Attorney-General, "Privacy Act Review Report", (2023), https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

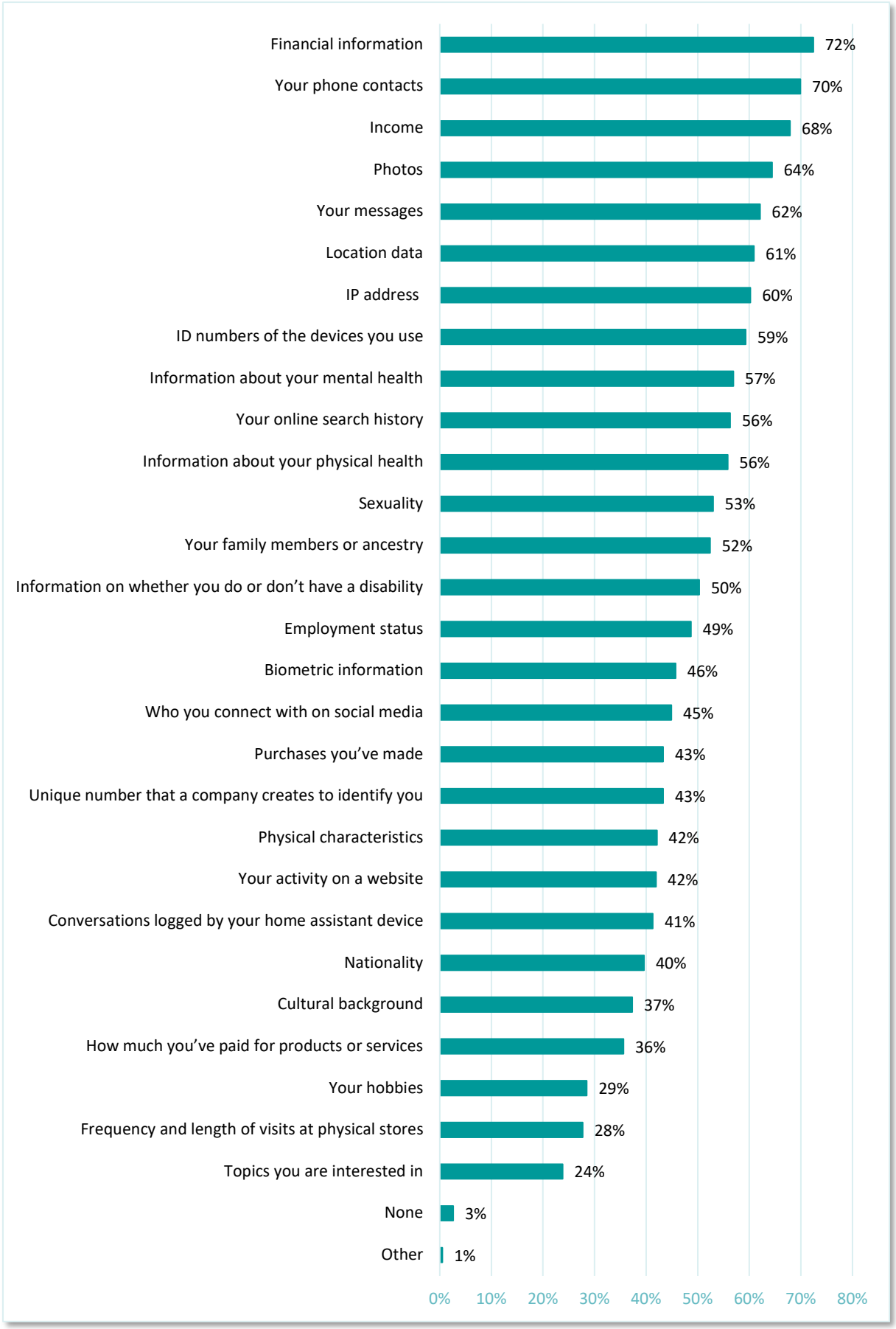


Figure 1: Consumer views on what constitutes personal information

Using personal information

The survey asked people if they are comfortable with how businesses use their personal information for specific activities (Figure 2). Australians showed high levels of discomfort with personal information being:

- used to create a personal profile (60% reported either very uncomfortable or somewhat uncomfortable)
- collected from other companies (69% reported either very uncomfortable or somewhat uncomfortable)
- used to develop a product or service that a consumer may be interested in (70% reported either very uncomfortable or somewhat uncomfortable)
- used to monitor their online behaviour (70% reported either very uncomfortable or somewhat uncomfortable)
- shared or sold with other companies (74% reported either very uncomfortable or somewhat uncomfortable).

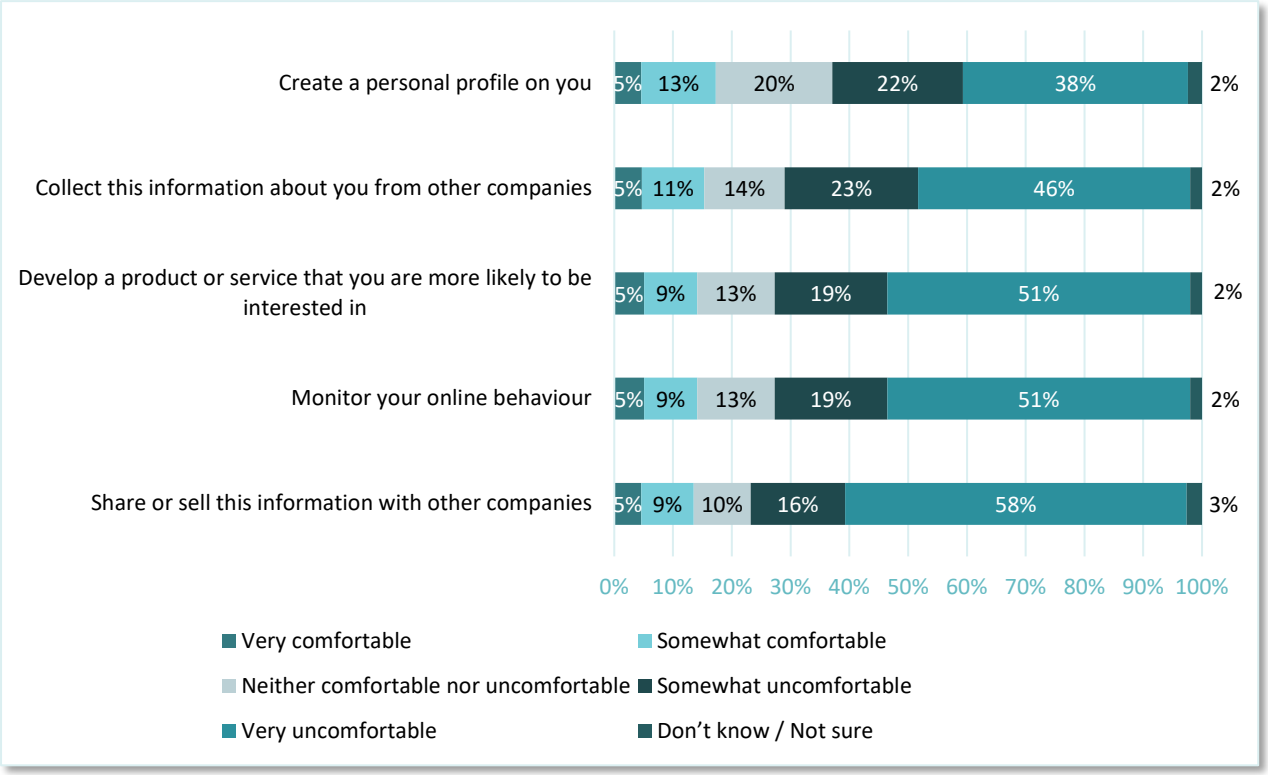


Figure 2: Comfort level with how personal information is used by businesses

"They are selling and or buying our data without being transparent about their practices. They are only concerned with themselves, profits, and how much they can sell to vulnerable people. They accomplish this by preying on consumers after being nosey about their details and targeting them. They are using our data to make more money for themselves whether we like it or not.

Comment from consumer survey participant

Consumer perceptions of privacy protections online

Placing the onus on consumers to protect their privacy is unfair when there is little responsibility placed on businesses to collect less data and use it safely. With 52% of consumers finding it time-consuming to protect their privacy online and 49% finding it frustrating, it's a recognition that current models and processes to privacy protection are failing to serve consumers adequately. Only 7% of consumers agree that companies give consumers real choices to protect their privacy online.

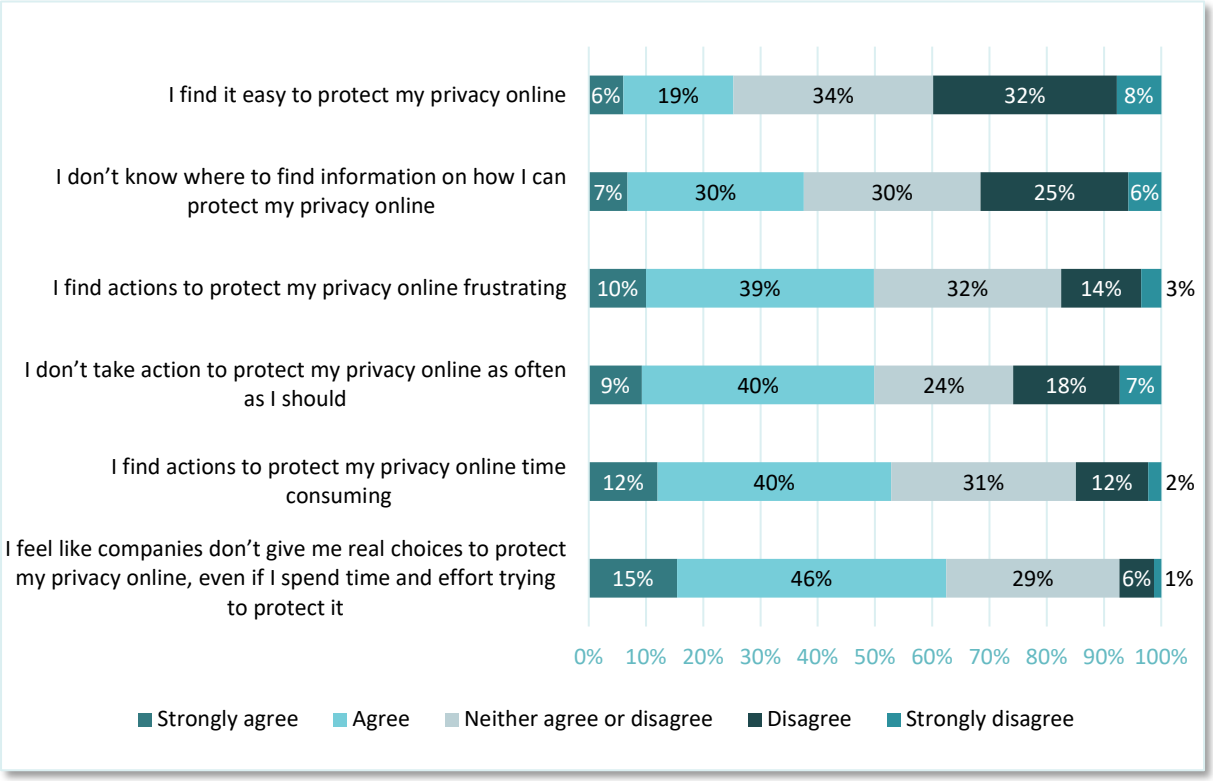


Figure 3: Consumer perception on protecting their privacy

Note: The option of 'Unsure' has been removed from this graph for ease of reading. It was 3% or less for each of the above options.

A sense of unfairness

Consumers reported finding several aspects of navigating privacy protections unfair (Table 1). These included:

- being required to accept a Privacy Policy that lets a company share consumer data with another company where it's not necessary to deliver the product or service (65% found it very unfair or unfair)
- difficulty finding the Privacy Policy (66% found it very unfair or unfair)
- being required to supply more personal information than is necessary to deliver the product or service (64% found it very unfair or unfair)
- lengthy and complex privacy policies (64% found it very unfair or unfair)
- website or app default settings are set to 'on' for all data collection and sharing that consumers must opt-out of (64% found it very unfair or unfair).

	Very unfair	Unfair
When you are required to accept a Privacy Policy that lets a company share your data with another company where that is not necessary to deliver the product or service	44%	21%
When it is hard to find the Privacy Policy that you are agreeing to about collecting and sharing your personal data	42%	24%
When companies require you to supply more personal information than is necessary to deliver the product or service	41%	23%
When options to reject or accept 'cookies' are difficult to find or require you to go to a third-party website	40%	25%
When the Privacy Policy is lengthy and complex in explaining how the company collects, uses and shares your personal data/information	37%	25%
When website or app default settings are set to 'on' for all data collection and sharing and you must opt-out	33%	26%

Table 1: Privacy actions and issues that consumers find unfair

Targeted advertising

When asked about targeted advertising, there was a clear discomfort with personal information being used without any baseline safeguards and limits on business practices.

Tracking online behaviour for targeted advertising

Only 9% of Australians reported being comfortable with companies targeting them with advertising based on their online behaviour even if they had not given permission (i.e., what a person may have previously viewed, searched for, purchased or discussed via a messaging app) (Figure 4).

Almost half (46%) of Australians are not comfortable with companies targeting advertising to them based on their online behaviour. Of those who were comfortable with targeted advertising (51%):

- 31% want to have the option to opt-out
- 25% only want to see targeted ads when they have opted-in
- 25% only want to see ads based on current search for product or service, and
- 17% were comfortable with companies targeting them with advertising even if they hadn't given permission (only 9% of the total population).

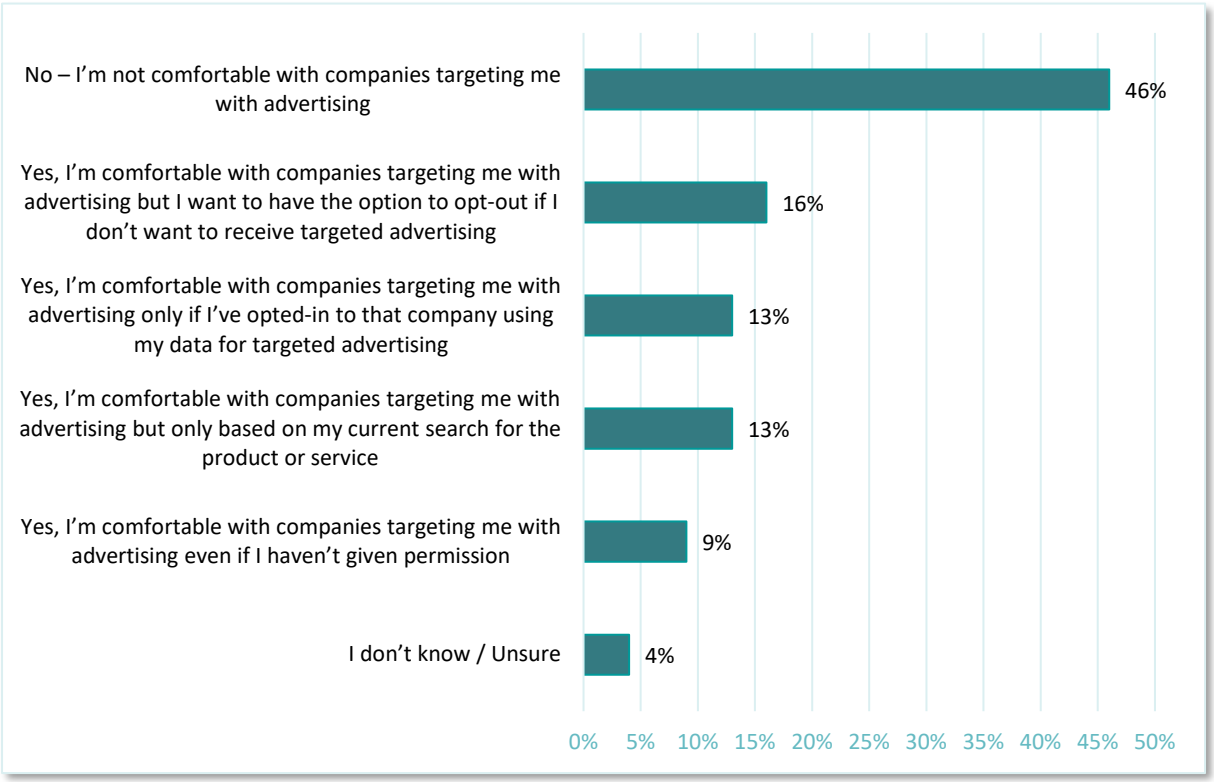


Figure 4: Level of comfort receiving targeted advertising based on online behaviour

"Why, after searching where to buy a car battery online, am I bombarded with endless ads from multiple suppliers for the next month even though I have already made my purchase?"

"I really feel annoyed when I search for products or services and then I start getting emails or suggestions within platforms for many months after."

Comments from consumer survey participant

Tracking personal characteristics for targeted advertising

Results are similar when it comes to targeted advertising based on personal characteristics (e.g., gender, age, income or location) (Figure 5). Only 8% of Australians reported being comfortable with companies targeting them advertising based on their personal characteristics even if they had not given permission.

Almost half (49%) of Australians are not comfortable with companies targeting advertising to them based on their personal characteristics. Of those who were comfortable (48%):

- 31% want to have the option to opt-out
- 29% only want to see targeted ads when they have opted-in
- 23% only want to see ads based on current search for product or service, and
- 16% were comfortable with companies targeting them with advertising even if they hadn't given permission (8% of the total population).

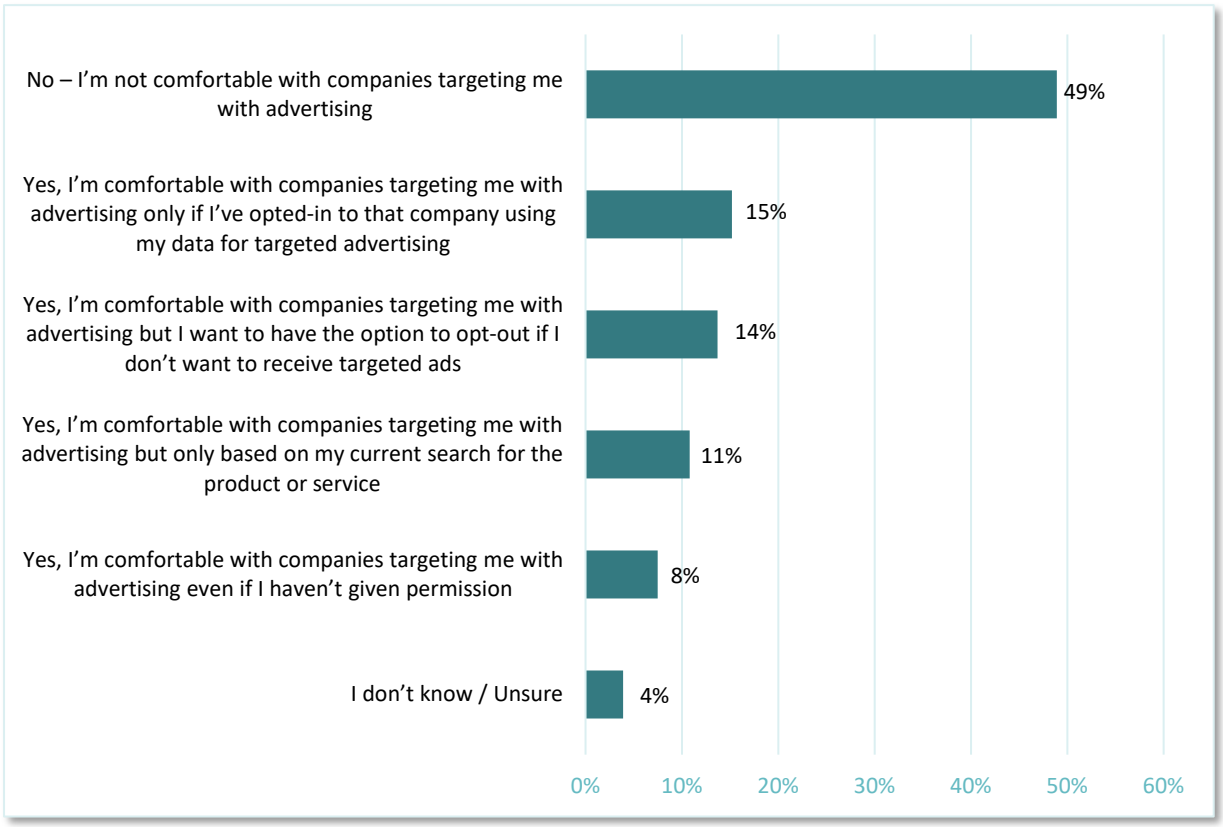


Figure 5: Level of comfort receiving targeted advertising based on personal characteristics

A very high percentage of Australians are uncomfortable with targeted advertising or would at least prefer that it is made available as an opt-in model. It is clear that an opt-in approach would be the safest option for Australians where the choice and control remain in their hands. Opt-in also should not mean that Australians are then subjected to dark patters / deceptive designs[4] including recurring notifications or nagging designed to coerce them into opting-in.

There is very limited consumer appetite to navigate the opt-out settings of the plethora of websites and apps that a person visits in a day.

> *"You really should have to opt in to all the various data sharing and mining. It shouldn't be a default."*
>
> Comment from consumer survey participant

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

Expectations of businesses

There is a gap between what consumers expect of businesses when it comes to privacy and what businesses are actually doing. When asked whether businesses are doing enough to protect consumer privacy, the resounding response was no (Table 2).

Businesses aren't doing enough	I'm satisfied that businesses are doing enough	Don't know / Not sure
70%	15%	16%

Table 2: Consumer views on whether businesses are doing enough to protect consumers' privacy

"I don't think they're working hard enough in protecting customer information these days."

"They are selling and or buying our data without being transparent about their practices."

Comments from consumer survey participant

Australians have much higher expectations of what good protections look like compared to what is currently on offer (Table 3). A high majority of the survey respondents (79%) agree that a company should only collect information that it needs to provide the product or service and 84% agree that data should be used with their interests in mind.

When it comes to selling and using data, the expectations are yet again high with Australians expecting more transparency on how their data may be used to assess their eligibility for a product or service (84%) and not wanting companies to sell their data under any circumstances (79%).

"Partner programs appear to be used as an excuse for information sharing as though within the same company."

"Many businesses collect all sorts of information before they will sell to you, I do not use these businesses, because I don't think that they need this information."

"I find that businesses collect data they don't need very often."

Comments from consumer survey participant

	Strongly agree	Agree
A company should only collect information about me that it needs to provide the product or service	46%	33%
A company should always act in my interests when it uses my data	54%	30%
A company should be transparent about how they use data about me to assess my eligibility for or exclude me from products or services	55%	29%
A company should give me clear and simple options to opt out of information they can collect, share or use about me	57%	28%
A company should not sell my data under any circumstances	58%	21%

Table 3: Percentage of survey respondents who either strongly agreed or agreed on what companies should and should not do

Business accountability

Most Australians believe businesses have the highest level of responsibility when it comes to how personal information is being collected, shared and used (Figure 6):

- 90% expect businesses to protect them against data misuse (i.e., data being used in a way that leaves people worse-off) (72% high; 18% moderate).
- 90% expect businesses to clearly explain how personal information is being used (71% high; 19% moderate).
- 88% expect businesses to ensure people are not opted-in by default for their data collection or sharing options (68% high; 20% moderate).
- 90% expect businesses to ensure people have access to opt-out from data collection, sharing and use options (69% high; 21% moderate).

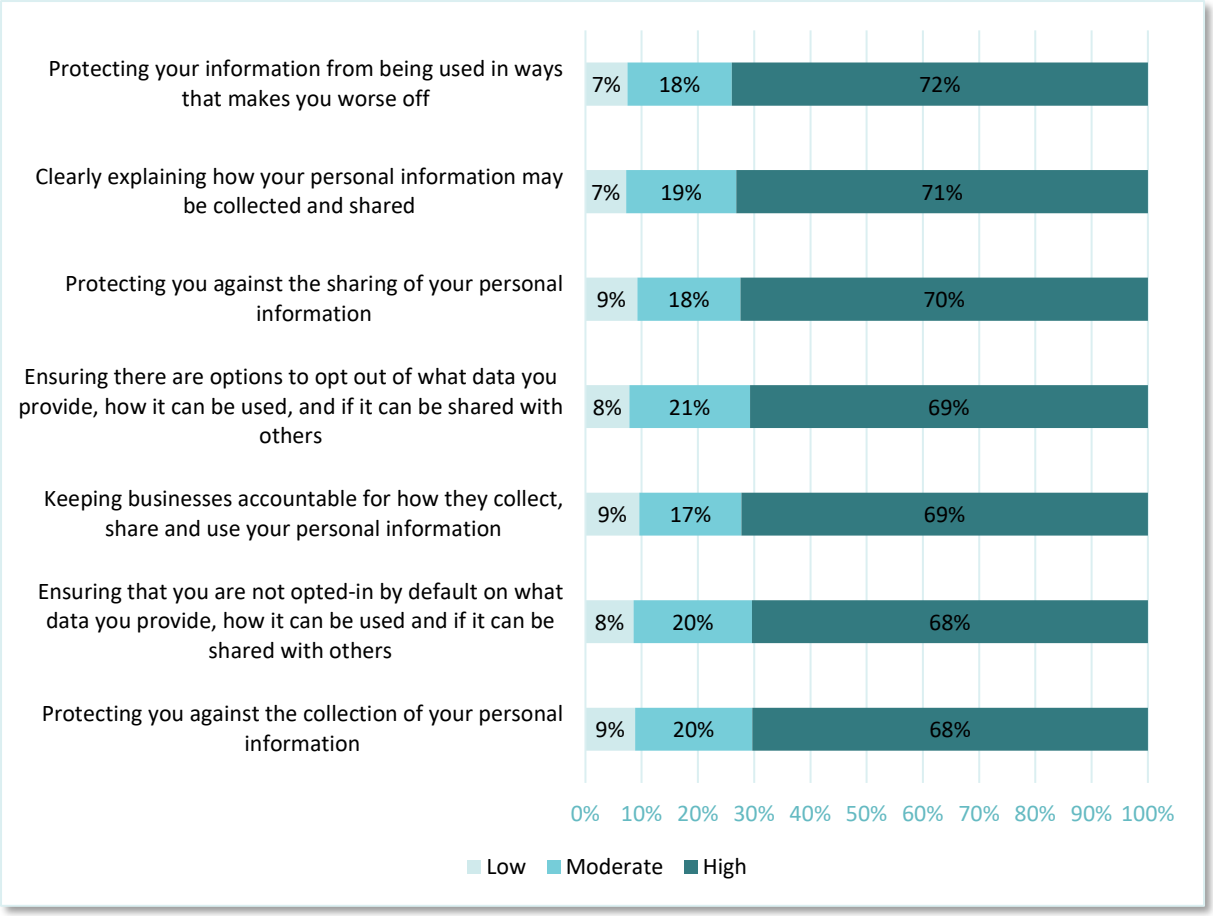


Figure 6: Consumer perceptions on level of responsibility for businesses when collecting, sharing and using consumer data
Note: The option of 'None/not relevant' has been removed from this graph for ease of reading. It was 4% or less for each of the above options.

Australians were asked what they think is a fair requirement on businesses that use their data (Figure 7). Most people thought it was fair to:

- require businesses to test and report the impact of their data practices on their customers or community before implementing them (57%), and
- request that a company delete personal information when it is no longer needed for the original purpose (73%).

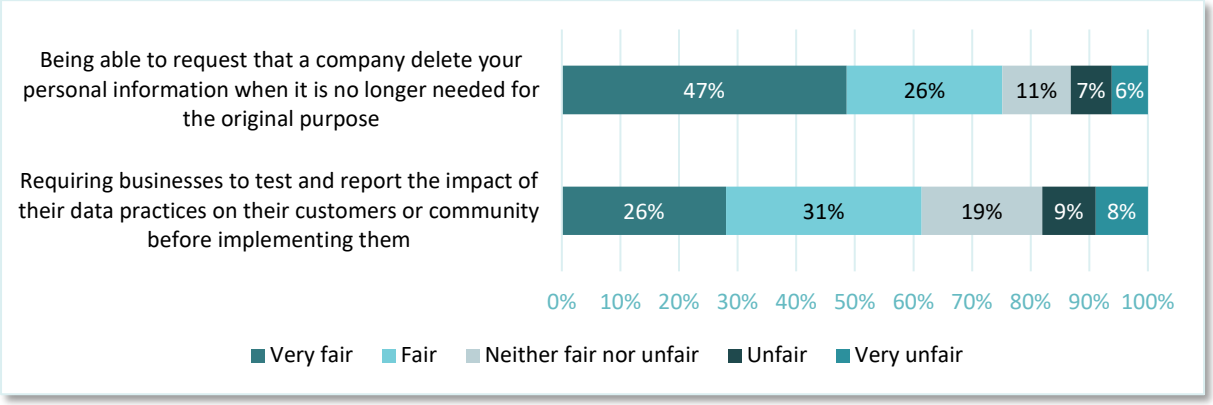


Figure 7: Consumer perceptions on protecting their privacy
Note: The option of 'Unsure' has been removed from this graph for ease of reading. It was 7% or less for each of the above options.

Expectations of small businesses

The size or nature of a business does not significantly influence what Australians expect from how their data is collected, shared and used (Figure 8). Similar to companies in general, Australians agree that small businesses should:

- not collect information that they don't need for delivering a product or service (81% for small businesses, 79% for all companies)
- not collect information about them that they don't currently need for delivering the product or service (81% for small businesses, 84% for all companies)
- not share or sell personal information to another organisation without a person's explicit consent (82% for small businesses, 79% for companies to not sell information under any circumstances)
- take steps to keep their personal information safe (82% for small businesses, 84% for all companies).

When it comes to collection of information, majority of Australians agree that small businesses should not collect personal information if they cannot ensure its safety and security (81%).

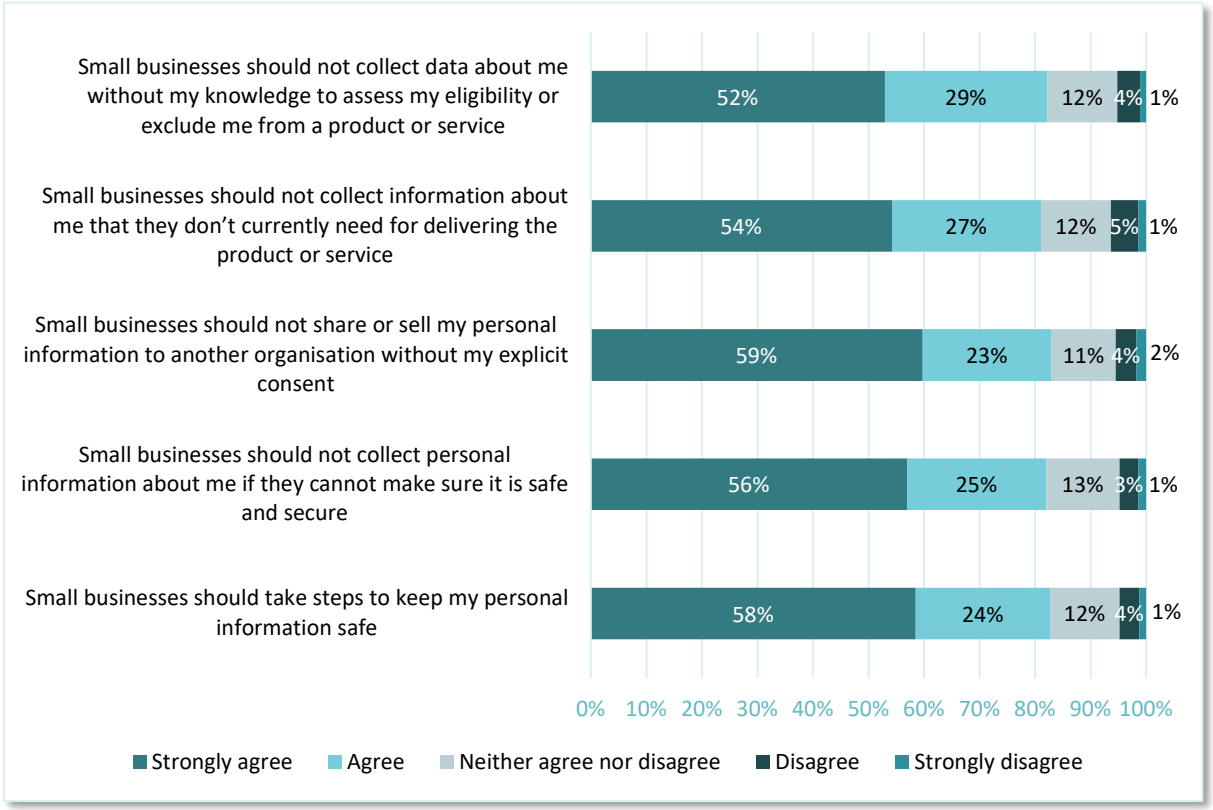


Figure 8: Consumer expectations of small businesses on privacy
Note: The option of 'Unsure' has been removed from this graph for ease of reading. It was 2% or less for each of the above options.

Using data for the right reasons

Australians acknowledge that there are instances when their personal information needs to be collected or shared without their knowledge but it is clear that those circumstances are limited (Figure 9).

Australians have a higher level of comfort if their personal information is being collected or shared to:

- guard against fraudulent use of a service (57% very comfortable to somewhat comfortable)
- prevent users who have previously been blocked from a service for misconduct from registering or using the service again (48% very comfortable to somewhat comfortable), and
- check your credit history when you apply for credit (42% very comfortable to somewhat comfortable).

The level of comfort shifts when personal information is being collected or shared to:

- more precisely conduct target advertising based on a person's attributes and interests, even without building a profile (51% uncomfortable)
- allocate people to a segment or group of customers based on information not provided directly to the company (49% uncomfortable), and
- create a more detailed profile on the person for marketing purposes (61% uncomfortable) or to share with other businesses (68% uncomfortable).

A significant portion of respondents noted that they were neither comfortable nor uncomfortable with various practices which indicates that there is potentially a lack of understanding of how personal information can be used and the impact of those use cases. It shows that relying on notification and consent as the primary consumer protection is not practical in a complex, data-driven economy.

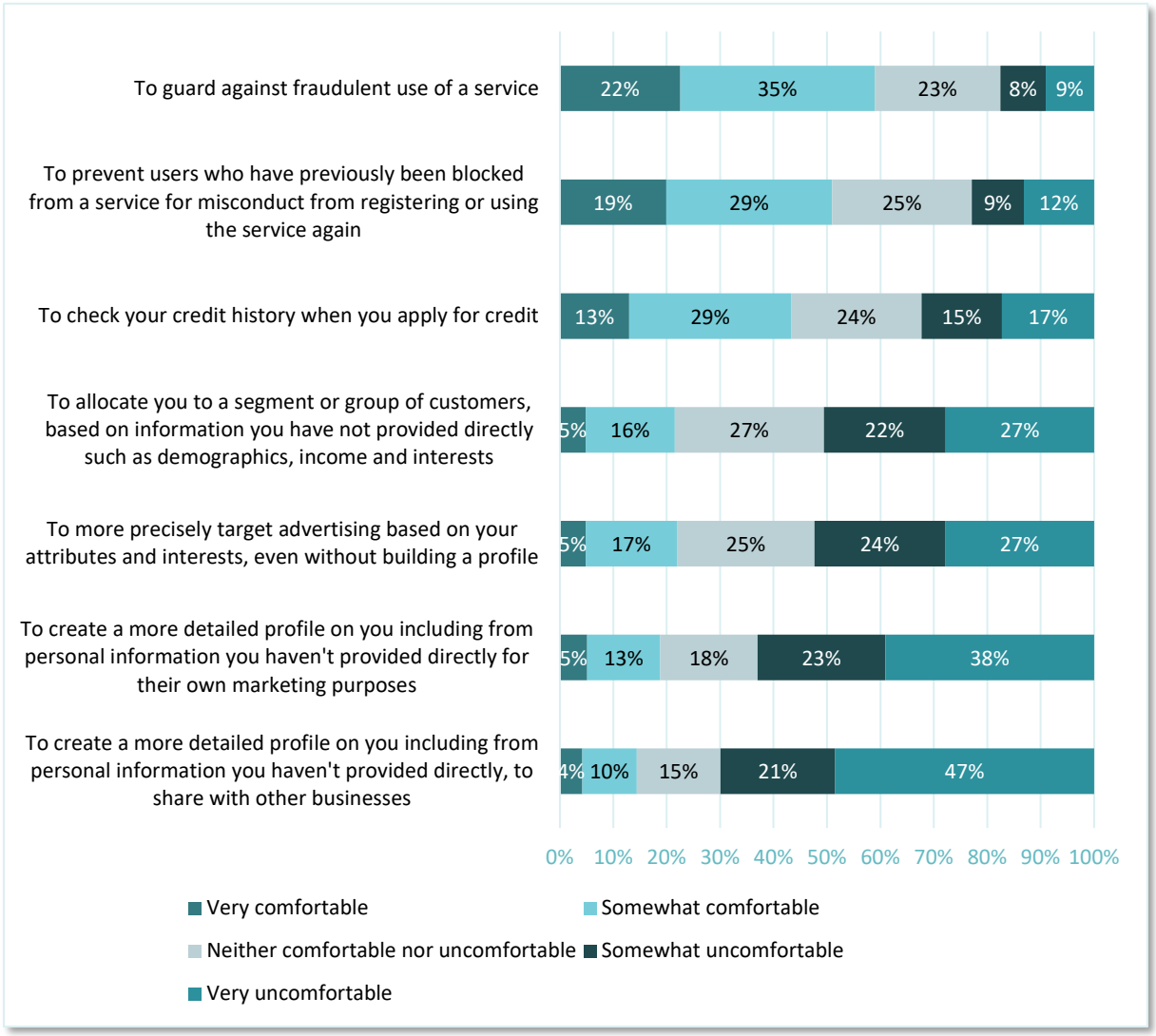


Figure 9: Consumer expectations on use of data without explicit consent
Note: The option of 'Unsure' has been removed from this graph for ease of reading. It was between 3% and 6% for each of the above options.

In the interest of the consumer

When people are sharing their personal information, they're expecting that it'll be used in their best interest and will not cause harm to them or others (Figure 10). Most Australians believe that:

- 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%)
- children's personal information should only be collected or used if it is in the best interest of the child and there is explicit consent from a parent or guardian (74%)
- 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%).

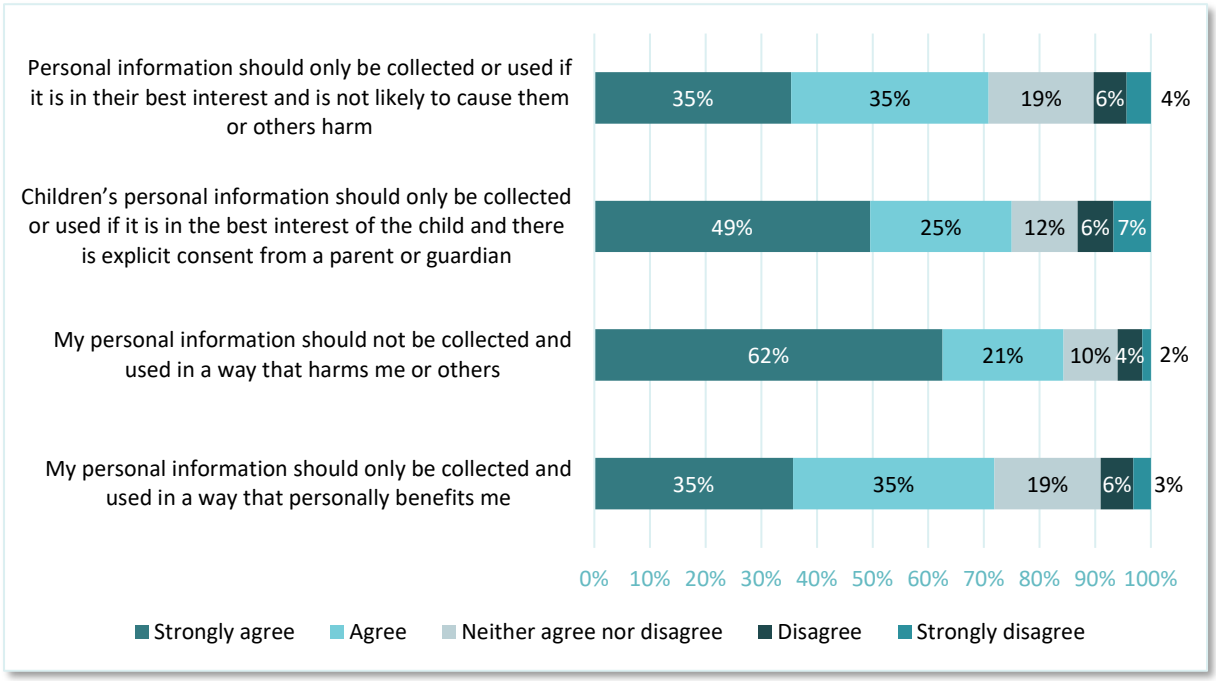


Figure 10: Consumer expectations on whose interest personal information is collected and used
Note: The option of 'Unsure' has been removed from this graph for ease of reading. It was 3% or less for each of the above options.

"Businesses don't care about protecting us, all they care about is making money. Prior to the internet they weren't able to collect personal information unless it was to deliver a service or product, and then it was just the delivery address. Just because we are all online DOES NOT MEAN we should have to sacrifice our personal data to be marketed to and have to put up with being slammed with ads or emails.

Comment from consumer survey participant

Keeping data safe

In light of Australia's high profile data breaches in late 2022[5], Australians were asked their views on businesses keeping their data safe (Figure 11). Regardless of the type of business, on average, close to half of Australians have little to no confidence that businesses will keep their data safe from future data breaches:

- Only 23% have some level of confidence in small businesses (44% are not confident).
- Only 25% have some level of confidence in large businesses (47% are not confident).
- Only 17% have some level of confidence in international businesses (57% are not confident).

The level of confidence erodes further with online only businesses, with, on average, close to 60% of Australians having little to no confidence with these businesses keep their data safe.

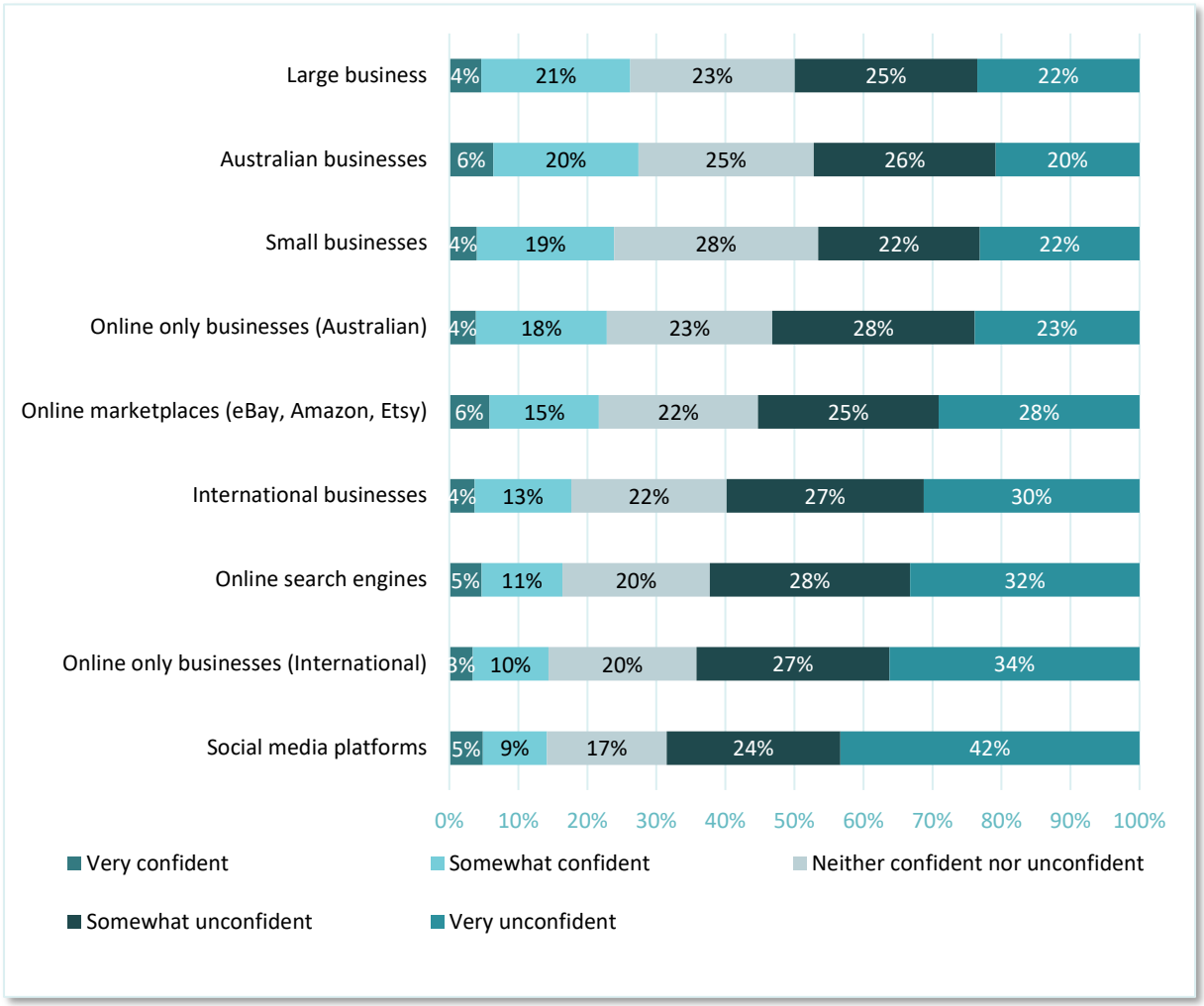


Figure 11: Consumer confidence in businesses to keep their data safe
Note: The option of 'Unsure' has been removed from this graph for ease of reading. It was 6% or less for each of the above options.

[5] Smith, P., "Cyber experts worry as Medibank puts hack behind it", (27 February 2023), Australian Financial Review, https://www.afr.com/technology/cyber-experts-worry-as-medibank-puts-hack-behind-it-20230223-p5cn10.

"The fact big businesses such as Optus and Medibank have been hacked does not fill me with confidence at all."

"15 years ago my son wanted a mobile phone so I had to give my personal information because he was a child. We closed the account 10 years ago and he took out his own policy with Telstra. Then when Optus was hacked he received a message (2 weeks later) advising his details had been hacked when it was actually mine - after the account had been closed for 10 years, this is totally deplorable and I should have been compensated most definitely."

Comment from consumer survey participant

When it comes to data protection, Australians expect far more than what they're getting (Table 4). To protect their data, Australians agree that a company should:

- delete personal information when it is no longer needed (83%)
- be responsible for keeping data safe (84%)
- protect them from harm if there is a data breach (65%)
- notify customers when there is a data breach and provide clear information about where to get help (86%).

	Strongly agree	Agree
A company should delete my personal information when it is no longer needed for the original purpose	61%	22%
A company who has my data should be responsible for keeping my data safe	61%	23%
A company should protect me from harm if my data is breached	62%	23%
A company should notify me when my data is breached and provide clear information about where to get help	62%	24%

Table 4: Consumer perception on protection against data breaches

Expectations of government

Most Australians believe government also has a high level of responsibility when it comes to how personal information is being collected, shared and used (Figure 12). Australians expect governments to protect them against data misuse (88%), clearly explain how personal information is being used (85%) and ensure consumers are not opted-in by default to data collection and sharing options (85%).

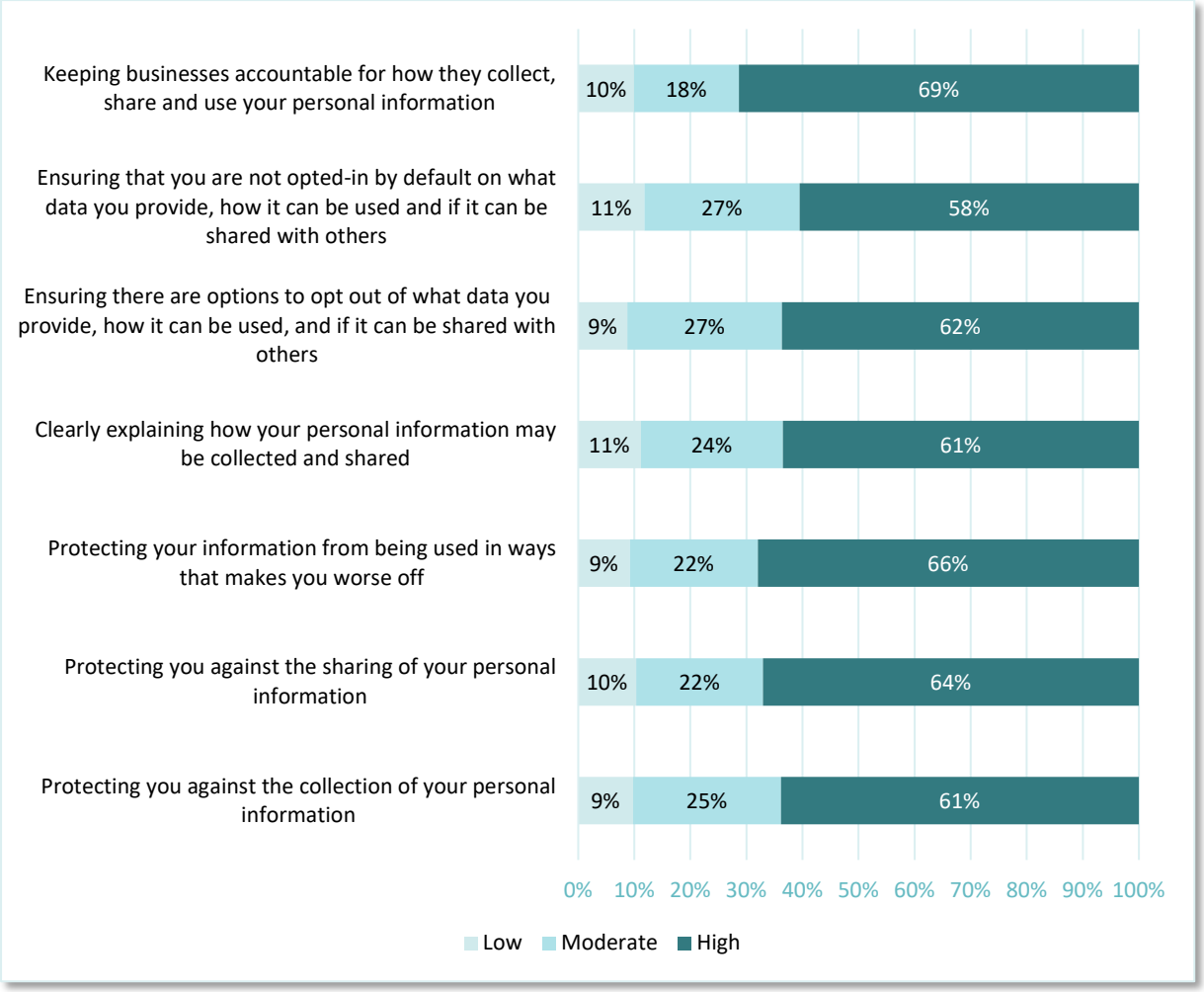


Figure 12: Consumer expectations of government
Note: The option of 'None/not relevant' has been removed from this graph for ease of reading. It was 4% or less for each of the above options.

Enforcing the law

In addition to valuing strong privacy protections, Australians also value strong enforcement and penalties (Figure 13). People consider it unfair that businesses can misuse consumer data without any enforcement or penalties imposed by the regulator (60% think it is unfair).

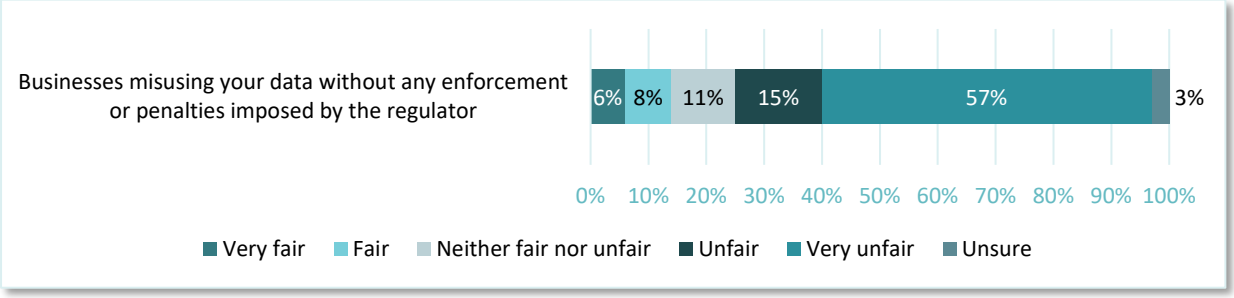


Figure 13: Measuring level of fairness for businesses misusing data without consequences

---

"When breaches happen no real solutions or preventative actions are put in place and no consequences are faced by the business."

"At the moment they have Carte Blanche to do as they please without being held to account."

Comments from consumer survey participant

Australians also consider that the regulator should have a range of mechanisms to hold businesses accountable (Figure 14). 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)
- the power to ban data practices that cause harm (81% strongly agree or agree)
- the ability to issue penalties for companies that breach privacy protections (82% strongly agree or agree).

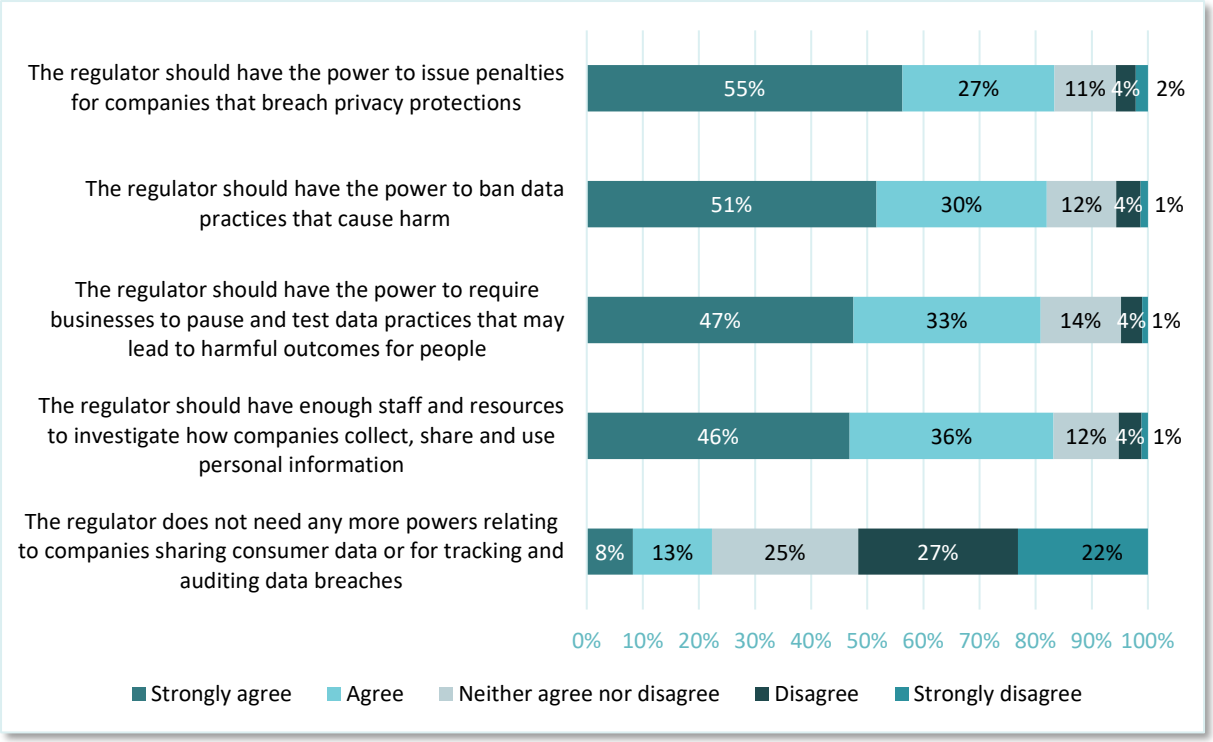


Figure 14: Consumer expectations of regulator powers

"Unless the law enforces privacy, it won't happen."

Comment from consumer survey participant

Support and redress

Australians are confused about who can help them or where they can get redress when something happens to their private information (Table 5):

- 50% do not know where to seek help if they have a problem with how a company collects, shares or uses their personal information.
- 46% do not know where to seek help if their data is hacked.
- 46% 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.
- 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.

	Strongly disagree	Disagree
I know where and who to seek help from if I have a problem with how a company collects, shares or uses my personal information	18%	32%
I know where or who to seek help from if I have had my data hacked	16%	30%
I know where or who to seek help from if I am being scammed	13%	23%
I know where or who to seek help from if I believe my personal information is being used in a way that is causing me harm (e.g., seeing ads targeted to me on a product that I am trying to quit)	16%	30%
I am confident I will be compensated if I have been left worse-off because of how a company collected, shared or used my data	5%	13%

Table 5: Consumer expectations of regulator powers