Consumer Policy Research Centre

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

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

1 December 2020

RESPONSE TO PRIVACY ACT REVEW ISSUES PAPER

The Consumer Policy Research Centre (CPRC) welcomes the opportunity to respond to the Australian Attorney-General's Department Privacy Act Review Issues Paper.

CPRC aims to create fairer, safer and inclusive markets by undertaking research and working with leading regulators, policymakers, businesses, academics and community advocates. Data and technology issues are a research focus for CPRC, including emerging risks and harms and opportunities to better use data to improve consumer wellbeing and welfare.

WHERE WE ARE TODAY

CPRC strongly agrees with the Australian Competition and Consumer Commission's (ACCC) finding that "*the Privacy Act needs reform in order to ensure consumers are adequately informed, empowered and protected, as to how their data is being used and collected*" and that such reforms will "*increase trust in the digital economy and spur competition between businesses on the basis of privacy*".[1] CPRC has a keen interest in how Australia's privacy protection framework can be reformed so it offers modern, robust protections that ensure Australian consumers, and our overall society, are better off as the Fourth Industrial Revolution[2] continues to gather speed.

As we have previously raised with government[3] – data-driven technology is being rapidly deployed across the Australian community without a coherent protection framework in place. This trend has intensified in 2020. We have seen consumption of data driven technology, products and services explode as a result of COVID-19 health restrictions – with more people working, learning, shopping, socialising and being entertained online than ever before. For many consumers this will be a permanent shift. At the same time government is seeking to accelerate digitisation through its Digital Business Plan and Consumer Data Right reforms – with a view to growing the economy post COVID-19 and ensuring Australia is a "world leading" digital economy and society by 2030.[4] This review of the Privacy Act – and the government's overall response to the ACCC Digital Platforms Inquiry Final Report – should be seen as an opportunity to ensure Australians can also benefit from a "world

[1] ACCC, "Digital Platforms Inquiry – Final Report", (June 2019), 3, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf
[2] World Economic Forum, "Fourth Industrial Revolution", (accessed November 2020), https://www.weforum.org/focus/fourth-industrial-revolution
[3] CPRC, "Submission by Consumer Policy Research Centre to Australian Treasury consultation on the ACCC Digital Platforms Inquiry Final Report", (September 2019), https://cprc.org.au/app/uploads/2019/09/DigitalPlatformsInquiry_CPRC2019_Final-1.pdf
[4] Prime Minister of Australia, "Digital Business Plan to Drive Australia's Economic Recovery", (September 2020), https://www.pm.gov.au/media/digital-business-plan-drive-australias-economic-recovery

leading" protections regime that enables innovation and drives fair, safe and inclusive outcomes for all consumers.

WHERE WE NEED TO BE

The government's economic growth and 2030 digitisation ambitions need to be matched by ambitious reforms of consumer protections. In our view, failing to take this approach in the face of rapid digitisation and technological change is an unacceptable gamble and we therefore urge government to be bold and innovative when reforming the Privacy Act. Our response to the Issues Paper utilises CPRC's research and evidence-based perspective to highlight areas where bold changes to the Australia's privacy protection framework would benefit consumers. Specifically, our response addresses:

1. **The scope of the Act** – the Act's coverage must be drastically updated so that it reflects the increasing ubiquity of data collection, use and disclosure in the economy[5]
2. **Transparency and comprehension** – privacy notices must be better at informing consumers about the collection, use and disclosure of consumer data
3. **Choice and control** – consent mechanisms need to provide consumers with more meaningful choice and control over their data
4. **Enforcement** – robust enforcement and remedial mechanisms must effectively hold entities to account and incentivise the right data-handling behaviours and culture
5. **Beyond analogue privacy protections** – modern laws and regulations must work coherently to protect the interests of Australian consumers.

We do not respond to all the questions set out in the Issues Paper but where we feel that a point is relevant to a specific question we denote this in the footnotes.

1. THE SCOPE OF THE ACT

1.1 Objects of the Privacy Act

There are well-documented challenges with technology restricting our human right to privacy in the digital era. These include the ease of collecting and using personal information with new technologies, quick and easy flow of data across borders and difficulties correcting or removing personal information once it is communicated.[6] Table 1 below outlines our views on how changes to some of the objects in Section 2A of the Privacy Act[7] could help to better-align the legislation with modern norms regarding privacy.

Table 1 – Changes to the objects of the Privacy Act

Existing object	Proposed amendment
"to recognise that the protection of the privacy of	A contractual approach to privacy regulation based on informed consent and "balanced" interests between individuals and entities implies that consumers can trade away or lose their human right to privacy in a range of circumstances where this benefits entities. We

[5] This trend is not new, with the White House releasing a report back in 2015 stating how "the declining cost of data collection, storage, and processing, coupled with new sources of data from sensors, cameras, and geospatial technologies, means that we live in a world where data collection is nearly ubiquitous, where data retention can be functionally permanent, and where data analysis is increasingly conducted in speeds approaching real time". See: Obama White House, "Big Data: Seizing Opportunities, Preserving Values – Interim Progress Report", (February 2015), 1-2, https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf

[6] Australian Human Rights Commission, "Human Rights and Technology – Discussion Paper", (December 2019), 18 https://humanrights.gov.au/sites/default/files/document/publication/techrights_2019_discussionpaper_0.pdf

[7] Refer to Question 1.

individuals is balanced with the interests of entities in carrying out their functions or activities"	believe that this is out of step with the expectations of Australians and more broadly with approaches taken to modern data policy developments internationally. In particular, it fails to recognise the very significant power imbalances between businesses and consumers. For example, businesses can have vast access to a growing scale and scope of information about Australians, and an increasingly sophisticated understanding of how to extract value from and monetise that information. At the same time, consumers currently experience a total lack of transparency, meaningful informed choice, and power in relation to a) how their data is collected, shared and used by others and b) the value of that data and how that data and personal information could and should be used in a way to improve their own welfare and wellbeing. Without broader and serious recognition of the significant structural changes underway in Australia and globally as a result of data extraction, digital transformation and AI – and addressing the significant power imbalances the current approach to privacy regulation has enabled – Privacy Act reforms are at risk of being perceived to be "just another update", rather than something that will have significant beneficial economic and social consequences for our nation and our community for years to come. This object should therefore be reframed so that it focuses on an **individual's right to privacy and emphasises that there is an onus on entities to protect and promote this right when handling an individual's data**.
"to promote responsible and transparent handling of personal information by entities"	Transparency of information alone does not itself provide meaningful protection to individuals in a world where data collection is ubiquitous. There needs to be more focus on what "responsible" actually means in the context of data-handling in the digital age. For instance, the object should emphasise the importance of treating consumers "**fairly**" and ensuring consumer "**safety"** is not put at risk. Reflecting this policy intent in the objects of the Act would help provide a clearer signal to entities about the standards of consumer data handling expected in Australia.
"to provide a means for individuals to complain about an alleged interference with their privacy":	For an individual to have the means to complain about a privacy issue or contest an outcome they would usually need to be able to understand what has happened to their information.[8] Therefore – we consider that also providing consumers with a means to "**gain a comprehensible explanation about the handling of their personal information**" is needed if consumers are to be able to complain about or contest an issue effectively.

1.2 Small business exemptions

Given the increasing role of data collection, use and disclosure across the Australian economy – and the government's efforts to accelerate this trend – we consider it is essential to extend the scope of the Privacy Act to more business by changing the small business exemption.[9] The ACCC estimates that 94% of Australian businesses are currently exempt

[8] The Alan Turing Institute, "A right to Explanation", (accessed November 2020), https://www.turing.ac.uk/research/impact-stories/a-right-to-explanation

[9] Refer to Question 7

from the Act.[10] We agree with the assertion in the Issues Paper that advances in technology and ways of doing business (since the current exemption was introduced) mean small businesses are increasingly handling the personal information of their consumers – and this comes with higher privacy risks.[11]

All businesses – large and small – that handle personal information should be captured by the scope of the Act, regardless of whether they have attained the consent of individuals to collect or disclose their personal information.[12] Safeguarding the privacy of consumers in such circumstances is paramount to fostering confidence and trust in an increasingly digitised economy. Just as businesses large and small have a responsibility - and bear costs for ensuring - the safety of consumers walking around their "bricks and mortar" stores, a cost of doing business in the digital age is ensuring consumers personal information and privacy is appropriately protected.

1.3 Definition of personal information

CPRC maintains strong support for the ACCC's recommendation 16(a) to update the "personal information" definition in the Privacy Act to clarify that it includes technical data such as IP addresses, device identifiers, location data and any other data that may be used to identify an individual.[13] CPRC's "*2020 Data and Technology Consumer Survey"* (see **Attachment 1**) asked consumers about the information consumers would be "uncomfortable with companies sharing with third parties for purposes other than delivering the product or service they'd signed up for". Of those surveyed 73% told us they would be uncomfortable with location data being shared, while 82% would be uncomfortable with unique mobile phone/device ID numbers being shared (the same level of concerned as sharing a home address and health information).[14] This reflects the extent to which, for many consumers, mobile phones are no longer simply functional communication devices but have become hubs and repositories for generating and storing extensive personal data. Consumers are worried about how the collection, use and disclosure of this information can present risks to their privacy. Ensuring such technical data is included within the definition of personal information in the Act will help to mitigate such risks. Failing to do so would be significantly out of step with community expectations and technological advancements.

1.4 Inferred information

Past research from CPRC has highlighted how common information now collected by companies such as device ID, location, usage behaviour, search history, messaging and communications content, relationships and contacts, biometrics, transactions and purchase interests can all be combined to develop very detailed inferred information and profiles.[15] This includes information such as socioeconomic status, sexual orientation, political views, mood, stress levels, health status, personal interests, customer worth or relationship status. As the Issues Paper notes, entities are effectively able to generate inferred personal and sensitive information about individuals without their knowledge or consent.[16] This status quo

[10] ACCC, "Digital Platforms Inquiry – Final Report", (June 2019), 458.
[11] Australian Government Attorney-General's Department, "Review of the Privacy Act 1988 (Cth) – Issues Paper", (October 2020), 24, https://www.ag.gov.au/integrity/publications/review-privacy-act-1988-cth-issues-paper
[12] Refer to Question 12
[13] Refer to Question 2
[14] Refer to p. 17 of the survey results report at Attachment 1 to this submission.
[15] Brigid Richmond, "A Day in the Life of Data", (May 2019), 6-12, https://cprc.org.au/app/uploads/2019/05/CPRC-Research-Report_A-Day-in-the-Life-of-Data_final-full-report.pdf ; Phuong Nguyen & Lauren Solomon, "Consumer Data and the Digital Economy", (July 2018), 6-9, https://cprc.org.au/app/uploads/2018/07/Full_Data_Report_A4_FIN.pdf
[16] Australian Government Attorney-General's Department, "Review of the Privacy Act 1988 (Cth) – Issues Paper", (October 2020), 45

undermines an individual's right to privacy and we therefore strongly support the prohibition of activities that infer personal information without the consent of a consumer.[17]

We note that the Issues Paper states that past survey results "*suggest Australians are split in their views about inferred personal information*" in the context of being profiled or inferring their tastes and preferences.[18] We strongly dispute this statement. CPRC's 2020 research found that 74% of Australian consumers have safety concerns in relation to being targeted with particular products or services (37% very concerned, 36% slightly concerned), 76% consider it to be unfair when their personal information is used to make predictions about them (47% very unfair, 29% unfair) and 80% consider it is unfair for their personal information to impact what products they are eligible for (54% very unfair, 26% unfair).[19] These strong consumer sentiments regarding safety and fairness hold – whether personal information is inferred or otherwise.

1.5 Protecting personal information from re-identification

Risks of consumer data being re-identified are well-documented.[20] Therefore, effective procedures and processes that safeguard personal and sensitive information from being re-identified are an essential component of privacy protections.[21] As a starting point – government should explore the merits of regulatory consistency with other jurisdictions in which, the Issues Paper notes, "personal information must be anonymised rather than de-identified for the definition of personal information (or personal data) to no longer apply".[22] This will help to ensure Australian consumers' are afforded equivalent levels of protection from risks of re-identification to consumers overseas, while also enabling firms in Australia to be more readily able to compete in jurisdictions where privacy protections are more aligned with modern technology. How frameworks that safeguard against re-identification of data[23] can be codified in law – so there is greater accountability for upholding appropriate protection standards – should also be explored.

2. TRANSPARENCY AND COMPREHENSION

2.1 Lack of engagement with current privacy policies

Evidence of the current shortcomings of privacy policies are extensive – with opacity, complexity, length and vagueness being some of the most glaring issues.[24] Given the extent of "concealed data practices"[25] privacy policies are currently failing at their stated aim as the:

"*basis for individuals to understand why an entity is collecting their personal information and to make an informed decision about whether to consent to a proposed collection of certain types of personal information and to the use or disclosure of their personal information for certain purposes*".[26]

---

[17] Refer to Question 35.
[18] Ibid, 19.
[19] Attachment 1, p. 25 & 27.
[20] For example, see: Brigid Richmond, "A Day in the Life of Data", (May 2019), 31 ; and Luc Rocher, Julien Hendrickx & Yves-Alexadre de Montjoye, 'Estimating the success of re-identifications in incomplete datasets using generative models'. (Nature Communications 10, 3069, 2019), https://www.nature.com/articles/s41467-019-10933-3
[21] Refer to Question 4
[22] Whereby "anonymisation is the process of irreversibly treating data so that no individual can be identified, including by the holders of the data". See: Australian Government Attorney-General's Department, "Review of the Privacy Act 1988 (Cth) – Issues Paper", (October 2020), 20
[23] We note that the existing de-identification decision-making framework released by Office of the Australian Information Commissioner (OAIC) is non-binding. See: Ibid, 20.
[24] Brigid Richmond, "A Day in the Life of Data", (May 2019), 25-33.
[25] Katharine Kemp, "Concealed data practices and competition law: Why privacy matters", (University of New South Wales Law Research Series , August 2019), 11-19, http://www5.austlii.edu.au/au/journals/UNSWLRS/2019/53.pdf
[26] Australian Government Attorney-General's Department, "Review of the Privacy Act 1988 (Cth) – Issues Paper", (October 2020), 37

Our consumer survey results from 2018 and 2020 (see **Attachment 1**) indicate that effective consumer engagement with the information in privacy policies and T&Cs documents has not increased since 2018.[27] Key findings from the survey include:

- Across both years of the survey only 6% of Australians reported reading privacy policies and T&Cs all of the time, 33% of consumers never read this information, and 35% only read it for a few products / services they sign up for
- Only 33% of consumers agreed that it is enough for businesses to notify them of data collection through privacy policies and T&Cs (down from 37% in 2018)
- 88% of consumer feel it is unfair when T&Cs are hard to find (61% very unfair, 27% unfair).

2.2 Strengthening privacy notice requirements

CPRC strongly supports ACCC recommendation 16(b) from the Digital Platforms Inquiry regarding the strengthening of privacy notice requirements.[28] To improve their effectiveness – we would particularly stress the need for regulation to require notices that are more concise and intelligible, so consumers are empowered to comprehend information important to understanding how their data is being handled. Depending on the circumstances, this information could relate to how their data is being used to influence or make predictions about them, or how their data is being shared with other entities. Knowing this information will help enable consumers to make informed, meaningful choices on this basis.[29] The Privacy Act needs to place a clear onus on firms – in particular those whose business models are predicated on the collection, use and disclosure of consumer data – to satisfy themselves that consumers are being enabled to make informed, meaningful choices. Stronger notice requirements within the Act should therefore incentivise entities to test, trial and innovate in how they convey important information to consumers. Layered notices, the use of standardised words and icons, and privacy certification schemes can all be explored as ways to limit information burdens and overload.[30]

We strongly agree with the ACCC that any additional regulatory burden[31] on firms from strengthening notification requirements is likely to be outweighed by the benefits.[32] Addressing existing market and regulatory failures by improving transparency and consumer comprehension regarding data handling will mean consumers will be better able to manage their privacy. This will drive more competition on the basis of fair, safe and responsible data-handling practices that respect consumer privacy.

2.3 Greater transparency of data collection practices

Consumers need support for maintaining awareness and control regarding how their data is being collected, used and disclosed. Instances where third party entities collect an individual's personal information without notifying the individual[33] can obviously lead to invasions of a consumer's privacy and exploitation. We therefore agree with the ACCC's view that an individual should always be provided with notice when their personal information is collected, regardless of whether the collection is direct or indirect via a third party.[34] Where this cannot be done – the personal information should not be collected.

[27] See Attachment 1, pp. 16-23.
[28] ACCC, "Digital Platforms Inquiry – Final Report", (June 2019), 35.
[29] Refer to Questions 21 and 22
[30] Refer to Questions 24 and 25
[31] Refer to Question 20
[32] Ibid, 462.
[33] Refer to Question 23
[34] Australian Government Attorney-General's Department, "Review of the Privacy Act 1988 (Cth) – Issues Paper", (October 2020), 39

Without such a requirement the trading of consumers' data will remain a free for all – with scant regard given to individuals' rights to privacy and the desire expressed by consumers to have visibility over their data.[35]

The ongoing lack of transparency of data practices hinders the ability of consumers, privacy and consumer advocates and regulators themselves to hold companies to account. Opacity also inhibits the ability of the policy and regulatory community to build a stronger appreciation and understanding of the operation of data-driven product and service markets and how these are evolving particularly as the primary fuel to AI. In order to achieve enhanced transparency and consumer visibility over the collection of personal data we would strongly encourage government to think beyond the existing Privacy Act construct, as only seeking to amend it may constrain the options available. Examples of initiatives that could be explored include:[36]

- Codifying **privacy and security by design principles**[37] in the Privacy Act so there are obligations on entities to embed these principles into their own data-handling practices.
- Establishing a legal framework for **Data Trusts**[38] that place binding fiduciary obligations on trustees to manage and exercise data privacy rights on behalf of individuals who can then simply and easily choose the level of privacy protection they are comfortable with.
- Ensuring individuals and communities have more of a say in how their data is used through **data sovereignty**[39] arrangements.

For the Privacy Act reforms to help set Australia up to be a world leading digital economy by 2030 we reiterate that it is essential that the Review consider a range of bold reforms that help to fundamentally address the information asymmetries, bargaining power imbalances and behavioural biases that characterise the current data handling landscape in Australia.

3. CHOICE AND CONTROL

3.1 Stronger consent requirements

CPRC strongly support the ACCC's recommendations regarding strengthened consent requirements.[40] As CPRC has raised in prior submissions, any consumer consent to data collection, use and disclosure must be voluntary, express, informed, specific to purpose, time limited and easily withdrawn.[41] This should be the standard across a broad range of data-handling contexts, including direct marketing.[42] We consider effective consent regulations are especially important in the context of consumers facing a choice about using

[35] CPRC's 2020 survey results (see Attachment 1, p. 25).show that:
- 83% of consumers find it unfair (52% very unfair, 31% unfair) for a company to collect information about them from other companies
- 85% find it unfair (59% very unfair, 26% unfair) for a company to share personal information they've provided with other companies
- 90% of consumers find it unfair (72% very unfair, 18% unfair) for a company to sell personal information they've provided to other companies.

[36] Refer to Question 45

[37] Brigid Richmond, "A Day in the Life of Data", (May 2019), 49-51 ; Privacy by Design Centre of Excellence, "The Seven Foundational Principles", (accessed November 2020), https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/

[38] Anouk Ruhaak, "Data trusts: Why, What and How", (November 2019), https://medium.com/@anoukruhaak/data-trusts-why-what-and-how-a8b53b53d34 ; Sylvie Delacroix & Neil D Lawrence, "Bottom-up Data Trusts: disturbing the 'one size fits all' approach to data governance" (November 2019), https://academic.oup.com/idpl/article/9/4/236/5579842

[39] 'Data sovereignty' is the management of information in a way that aligns with the laws, practices and customs of a nation-state in which it is located. See: Matthew Snipp, "What Does Data Sovereignty Imply: What Does It Look Like?", in Tahu Kukutai and John Taylor (eds), "Indigenous Data Sovereignty: Towards an Agenda", (Canberra: ANU Press, 2016) 39-55.

[40] See recommendation 16(c) in: ACCC, "Digital Platforms Inquiry – Final Report", (June 2019), 35.

[41] CPRC, "Submission by Consumer Policy Research Centre to Australian Treasury consultation on the ACCC Digital Platforms Inquiry Final Report", (September 2019), 9.

[42] Refer to Question 37.

a product or service without a monetary charge – with the trade-off being that their data (and the predictions that can be drawn from it) are being monetised. We agree strongly with the assertion in the Issues Paper that, in the context of this trade-off, it is important that the individual has a proper understanding of the purposes for which their personal information may be used and disclosed and that their consent to such an arrangement is informed and meaningful.[43]

Transparency and genuine consumer control must be at the heart of reform to consent requirements. CPRC's consumer survey research (see **Attachment 1**) found that consumers do not currently feel either well-informed, or in control of their personal information:

- Only 6% of Australians are comfortable with how their personal information is collected and shared
- Only 12% of Australians report having a clear understanding of how their personal information is collected and shared
- Consumer discomfort with accepting privacy policies and T&Cs has grown, with 69% of 2020 survey respondents who had read such information in the past year accepting it for at least a few products or services despite feeling uncomfortable doing so – up from 67% in 2018. The vast majority did so because it was the only way to access the service (75%).

An effective notice and consent regime must ensure that consumers can make more informed choices about the services they choose to engage with by ensuring consumers:

- Can clearly understand what is being proposed with their data (which entities, for what purposes, for how long), and
- Are being provided with genuine options to accept or reject proposed data practices.

We also, however, strongly caution policymakers on over-reliance on consent and choice in the absence of protections which ensure safety and fair treatment. Safety and fairness should not be left to choice – these are things which consumers expect the law to ensure regardless of choice. The plethora of literature, including from the Australian Securities and Investments Commission[44], highlighting the risks of over-reliance on disclosure and "choice" (especially in complex or opaque markets) underscores how industry has increasingly made a mockery of the notion of helping consumers make informed decisions. Advancements in behavioural science and digital transformation has left consumers more vulnerable than ever to a range of practices which obscure meaningful choice, including deliberate "concealed data practices"[45] and "dark patterns"[46] that exacerbate information asymmetries and undermine consumer autonomy.

[43] Australian Government Attorney-General's Department, "Review of the Privacy Act 1988 (Cth) – Issues Paper", (October 2020), 43

[44] Australian Securities and Investments Commission & Dutch Authority for the Financial Markets, "Disclosure: Why it shouldn't be the default", (October 2019), 12, https://download.asic.gov.au/media/5303322/rep632-published-14-october-2019.pdf

[45] Katharine Kemp, "Concealed data practices and competition law: Why privacy matters", (University of New South Wales Law Research Series, August 2019), 11.

[46] Stigler Center for the Study of the Economy and the State, "Stigler committee on Digital Platforms – Final Report", (September 2019), 12, 237-257,https://research.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf?la=en&hash=2D23583FF8BCC560B7FEF7A81E1F95C1DDC5225E

3.2 Pro consumer defaults

Previous CPRC research outlines the strong impacts of defaults and status quo bias which anchor consumers to certain activities or providers.[47] The growing trend of bundling technology with particular platforms, apps or search engines presents significant issues for competition policy if consumers are anchored and defaulted to certain providers. We strongly support defaults for data sharing to be set to off to enable consumers to make active choices about disclosing their data.[48] Pro consumer defaults should also be supported by protections[49] that mean firms cannot preclude access to a good or service if a consumer refuses to consent to the unnecessary collection of their personal information.[50] Regulations that support informed and meaningful consent will help to boost consumers' knowledge of what they are consenting to and stimulate competition on the basis of privacy.[51] How such consent is asked for – and in what circumstances – needs to be based on robust research and user testing in order to manage challenges of consent fatigue.[52]

3.3 Right to erasure

CPRC supports consumers being given the right to erase their personal information and data held by companies where there is not a legal reason for it to be retained.[53] CPRC's 2020 consumer survey found that 89% of consumer considered such a right to be fair (71% very fair, 18% fair). We also agree with the ACCC that a right of erasure is a critical complement to strengthened consent requirements because it provides consumers with a mechanism for withdrawing their consent if they are no longer comfortable with an entity collecting, using or sharing their personal information. Without any capacity to require their data to be erased, consumers are not in a strong bargaining position with firms when it comes to the collection, sharing and use of their data. This is especially so when it comes to potential future uses of that data, because the value of data changes through time with the technology that is applied to it. A right to erase would ensure consumers have the ability to have their data deleted if they suspect it is being used for a different purpose to what they had originally signed up for.

[47] For example, see: Ben Martin Hobbs & Emma O'Neill, "The experiences of older consumers: towards markets that work for people", (July 2020), 50, https://cprc.org.au/publications/the-experiences-of-older-consumers-towards-markets-that-work-for-people/ ; Lauren Solomon & Ben Martin Hobbs, "Five preconditions of effective consumer engagement – a conceptual framework", (April 2018), 18 https://cprc.org.au/app/uploads/2018/04/Preconditions_Full_Report.pdf

[48] Refer to Question 32.

[49] Refer to Question 29.

[50] When asked what level of responsibility government and companies have for "ensuring options to opt out of what data consumers provide, how it can be used, and if it can be shared with others" 68% of consumers considered government has a "high" level responsibility for ensuring this, and 85% thought companies also have a "high" level of responsibility for ensuring this. See Attachment 1, p. 32.

[51] CPRC's 2020 consumer survey (Attachment 1, p. 25) shows that 82% of consumer find it unfair when default settings are set to "on" for all data collection and sharing (49% very unfair, 33% unfair). Mandating what pro privacy defaults look like in data-handling contexts – through the Act or associated regulatory tools – would therefore align with consumer expectations regarding protecting their right to privacy and allowing them to make affirmative decisions about how their data is collected, used and disclosed (in section 5.2 we set out some minimum standards that we consider should always be maintained).

[52] Refer to Question 28 and 30. We note that under the Consumer Data Right scheme the Data Standards Body undertakes consumer experience research and testing on a range of key issues, including consents. See: https://consumerdatastandards.gov.au/engagement/reports/reports-cx/

[53] Refer to Question 46.

3.4 Mandatory deletion of information that leads to risks

We consider it is important that a mandatory deletion mechanism be explored for personal information that relates to consumer vulnerabilities[54] or is sensitive[55]. While the ACCC noted that mandatory deletion could create a significant regulatory burden for small businesses only partially operating in the digital space[56] we do not consider it would be a disproportionate burden for firms handling data relating to highly personal information about an individual that could be used in ways that leave them worse off.[57] This would help to overcome behavioural biases (such as the "status quo" bias) that can prevent people requesting the deletion of information. We appreciate that such a requirement would need to be carefully designed so that it did not create circumstances where the deletion of such data could disadvantage a consumer or contradict other lawful reasons for holding data.

4. ENFORCEMENT

4.1 Consumer rights to action and redress

CPRC continues to support the Privacy Act reforms, recommended by the ACCC, regarding the introduction of a direct right of action for individuals (Recommendation 16(e)) and the introduction of a statutory tort for serious invasions of privacy (Recommendation 19). We consider both reforms will help to strengthen the rights and bargaining power of consumers when it comes to handling their data and exercising their right to privacy.[58]

Furthermore, we have also had the opportunity to read the Financial Rights Legal Centre (FRLC), Consumer Action Law Centre (CALC) and Financial Counselling Australia (FCA) joint submission to this review. We strongly support the view that individuals be given a right to bring actions and class actions against APP entities directly to court to seek compensation for financial and non-financial damages. We also recommend consideration of the Australian Financial Complaints Authority model for ensuring access to justice. Finally, we also note the benefit of more broadly establishing a digital ombudsman scheme to support consumers as they increasingly grapple with a range of harms associated with digital marketplaces.

4.2 Notifiable data breaches scheme

We consider that a mandated Notifiable Data Breaches Scheme is a regulatory tool that is important for a) ensuring consumers are aware when their privacy may be compromised, and b) driving improvements in transparency, accountability and compliance regarding how companies uphold their privacy obligations. To enhance the scheme's ability to drive such outcomes, the Review needs to consider whether the current 30 day timeline for reporting a breach to the OAIC sets an appropriate standard of transparency, accountability and compliance with privacy obligations. The Issues Paper highlights that the timeframe for reporting high risk breaches within the GDPR is 3 days, not 30 days.

---

[54] For example, this could relate to a consumer's income levels, ethnic background, income levels, whether they have a disability, whether they have a serious or chronic illness or come from a remote or indigenous community. See: Emma O'Neill, "Exploring Regulatory Approaches to Consumer Vulnerability", (November 2019), Chapter 2. https://cprc.org.au/app/uploads/2020/09/Exploring-regulatory-approaches-to-consumer-vulnerability-A-CPRC-report-for-the-AER.pdf

[55] This could relate to information about a person's socioeconomic status, sexual orientation, political views, personality, mood, stress levels, health, personal interests, consumer worth or value or relationship status. See: Brigid Richmond, "A Day in the Life of Data", (May 2019), 15.

[56] ACCC, "Digital Platforms Inquiry – Final Report", (June 2019), 473.

[57] Refer to Question 44.

[58] Refer to Questions 56 and 57.

We also consider that greater transparency, accountability and compliance improvements could be made if the OAIC were made aware of "less serious" instances that may indicate systemic data-handling and security issues within an entity. Reporting of such instances would be particularly proportionate for companies solely set up to handle consumer information, or who handle sensitive consumer data. This could assist OAIC in carrying out risks-based engagement and compliance activities that help prevent serious breaches from occurring in the first place.

4.3 Resourcing of regulators and consumer organisations

Nimble, focused and well-resourced regulation and enforcement regarding data-handling practices is essential to the consumer interest. Technology is moving much faster than policymakers and regulators are able to keep pace, and the speed of change means that the scope for significant and swift consumer harm is escalated. Given this context, CPRC[59] has previously stressed that government needs to ensure there is appropriate funding of regulators – and indeed the consumer organisations engaging on policy and regulatory issues.[60] This is needed so that the consumer interest is appropriately reflected in a wide range of important and complex regulatory and policy debates. To illustrate the current regulatory and policy landscape consumer organisations are operating in, CPRC has engaged with 17 agencies on data and technology reforms over the past 3 years. Concurrent to participating in this Privacy Act review – and maintaining our own research and policy program – CPRC is also actively participating in other reform processes concerning data and technology, which include (but are not limited to):

- Consumer Data Right reforms in both the finance and energy sectors
- Proposed reforms to the Australian Consumer Law regarding the prohibition of unfair trading practices and contract terms, and the addition of a general safety provision
- Ongoing work from the ACCC Digital Platforms Inquiry in relation to the ad tech sector and digital platform services
- the Data Availability and Transparency Bill legislation.

5. BEYOND ANALOGUE PRIVACY PROTECTIONS

5.1 Limitations of the traditional privacy regulation

CPRC recognise the shortcomings of the "notice and consent" model of privacy regulation[61] in a world where consumers are engaging with potentially hundreds of different products and services each day.

We consider there are three key shortcomings that limit its value:

- Firstly – placing an onus on consumers to read, comprehend and decide about giving consent for each data collection, sharing and use notice they encounter is not feasible. CPRC's 2020 "*Towards Markets that Work for People"* research report[62] highlights how effective information disclosure is often not enough to drive informed choices from

[59] CPRC, "Submission by Consumer Policy Research Centre to Australian Treasury consultation on the ACCC Digital Platforms Inquiry Final Report", (September 2019), 17.
[60] Refer to Question 53.
[61] Refer to Questions 20 and 26
[62] Ben Martin Hobbs & Emma O'Neill, "The experiences of older consumers: towards markets that work for people", (July 2020), 40 – 44.

consumers, and that choices are encumbered by "bounded rationality".[63] Further, research highlights the absurdity of requiring consumers to read all policies that apply to them in today's modern age. For example, one study concluded it would take an individual 244 hours per year (average of 40 minutes a day) to read all privacy policies that apply to the websites they visited.[64]

- Secondly – in addition to the above challenges regarding consumers being unable to make meaningful choices for every decision they face online, there is also the challenge of sufficient resourcing of enforcement bodies to identify and act on non-compliant and misleading consent notices. The scale of data collection in the Australian economy, and indeed the interconnected international economy, makes this a very challenging proposition.
- Thirdly – consumers are at a significant disadvantage when making choices about trade-offs relating to their data, because they cannot possibly foresee the potential future use, value or risk of that kind of data. Some data will be incredibly valuable with advancements in AI, other data may be less so. By forcing consumers into a situation where they "decide once" but bear the consequences potentially for the remainder of their life is not a fair trade. This starkly contrasts with the knowledge and capability of firms to understand the value and potential use of data. Power imbalances between firms and consumers are significant and cannot be ignored by this reform process. Power imbalances even between firms and regulators themselves are of increasing concern, with industry able to move much faster than policymakers in deploying technology that has the capacity to do significant harm.

So, while the notice and consent model of privacy regulation remains an important tool for enabling transparency and choice, the above shortcomings are to some extent intractable in the current era. Therefore, a "notice and consent" regulatory model should not be relied upon alone to ensure that consumers are sufficiently protected. The burden and responsibility must rest with businesses to ensure that consumer privacy is respected, that they do not cause harm through misuse or mishandling of personal information, and that consumers receive fair treatment. The notice and consent regulatory model must therefore operate alongside other protections that prohibit data collection, handling and use practices that are not in the consumer interest and can lead to detriment. We highlight as good practice two core principles set out as part of the Consumer Data Right: 1) that consent should be as easy to withdraw as it is to provide; and 2) the "Data Minimisation Principle" (i.e., that companies should not seek to collect more data than is specifically needed to fulfil their service to the consumer). Furthermore, Privacy Act reforms must be considered alongside reform to consumer law including the prohibition of unfair trading practices and contract terms, and the introduction of a general safety provision. In an increasingly complex and profitable digital economy characterised by the concentration of power in the hands of the few, it is up to government to ensure that market actors are the ones responsible for ensuring that the products that they sell in the marketplace respect human rights and meet minimum standards and expectations for safety and fairness.

5.2 Direct regulation of use and disclosure

We welcome the Issue Paper seeking comment on the direct regulation of data-handling practices, such as through the establishment of "no go zones".[65] CPRC holds the view that

[63] "Bounded Rationality" is the theory that individuals have a limited capacity to assimilate and digest all the information required to make perfectly rational decisions See: Herbert Simon, "Models of bounded rationality", (Cambridge, MA, MIT Press: 1982).

64 Aleecia McDonald & Lorrie Cranor, "The cost of Reading Privacy Policies". (I/S: A Journal of Law and Policy for the Information Society 2008 Privacy Year in Review), 4(3), http://www.aleecia.com/authors-drafts/readingPolicyCost-AV.pdf

[65] Australian Government Attorney-General's Department, "Review of the Privacy Act 1988 (Cth) – Issues Paper", (October 2020), 48.

some types of personal information and data are highly valuable, sensitive and may simply not be something we are comfortable as a society with trading away. We restrict trade in other areas where we believe there to be significant scope for harm and discrimination, for example, alcohol, narcotics and gambling. We consider there are certain kinds of data collection, use and disclosure practices that drive too much of a power imbalance or creates scope for discrimination and harm, particularly for minors or other people experiencing vulnerability.[66] To ensure such data-handling practices are not a feature of a highly digitised Australian economy direct regulatory interventions are required. As a starting point, CPRC suggests that the Review consider how to prohibit data-handling practices that leverage the following types of personal information (either actual or inferred) in ways that have been shown to cause harm and discrimination:

- a person's emotional stress[67] or mental health[68] circumstances
- a person's physical health and likelihood of disease[69]
- a person's inexperience in a market and potential financial vulnerability[70]

We recognise that balancing the need to protect consumers while also avoiding undue impacts on the legitimate uses of personal information is not a simple task. We also note the challenges associated with data that acts as a proxy for these attributes as opposed to direct collection of the attributes themselves. Careful consideration must be given as to whether tighter controls must be placed at the point of data collection, at the point of sharing, or in the application and use of this information. For these reasons, CPRC continues to strongly recommend that government and industry undertake further research (with civil society and academia where appropriate) in order to establish what kinds of data collection, sharing and use practices present significant risks of harm and discrimination to consumers.[71]

The value of such research can be seen in the recently released technical paper "*Using AI to make decisions: Addressing the problem of algorithmic bias"*.[72] This research – which was led by the Australian Human Rights Commission (AHRC) in collaboration with partners Gradient Institute, CPRC, Choice and CSIRO's Dat61 – shows how the use of consumers' data in AI systems risks being subject to algorithmic bias that can lead to consumers being unfairly treated, or even suffering unlawful discrimination. The paper offers guidance to companies on the steps they should take to avoid such risks. This is in line with community expectations, with a large majority Australian's considering that both government (79%) and companies (82%) have a high level responsibility in protecting their information from being used in ways that make them worse off.[73]

We also recognise that getting the aforementioned balance right will hinge on laws and regulations sending a clear signal to entities of what is expected in a range of data handling circumstances. An enforceable broad principle similar to Canada's Personal Information and Protection and Electronic Documents Act that sets an expectation that "*an organisation may collect, use or disclose personal information only for purposes that a reasonable person*

[66] Refer to Question 42
[67] Andrew Hutchinson, "On Facebook's Emotional Ad Targeting, the Manipulation of Younger Users, and the Concerns of Big Data", (May 2017), https://www.socialmediatoday.com/social-networks/facebooks-emotional-ad-targeting-manipulation-younger-users-and-concerns-big-data
[68] ABC News, "Insurers gaining 'open-ended access' to medical records slammed as 'unfair privacy breach'", (January 2019), https://www.abc.net.au/news/2019-01-24/medical-records-handed-to-insurance-companies-over-mental-health/10720024
[69] Phuong Nguyen & Lauren Solomon, "Consumer Data and the Digital Economy", (July 2018), 23.
[70] Vivien Chen, "Online Payday Lenders: Trusted Friends or Debt Traps?". (UNSW Law Journal, Volume 43(2), 2020), 675, http://www.unswlawjournal.unsw.edu.au/wp-content/uploads/2020/06/10-VIVIEN-CHEN.pdf
[71] CPRC, "Submission by Consumer Policy Research Centre to Australian Treasury consultation on the ACCC Digital Platforms Inquiry Final Report", (September 2019), 10.
[72] AHRC, "Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias", (November 2020), https://humanrights.gov.au/sites/default/files/document/publication/ahrc_technical_paper_algorithmic_bias_2020.pdf
[73] See Attachment 1, p. 30.

would consider appropriate in the circumstances" could be a useful basis for such a signal.[74] This could then be supported additional narrower principles, specific prescriptive rules and guidance that defines what is expected and/or prohibited in different circumstances.

5.3 The broader data governance and protection framework in Australia

Privacy protections overlap significantly with areas of law and regulation that promote consumer interests – such as consumer law, competition law, and human rights law. Australian policymakers and regulators need to be focused on how these broad protections interact[75] – and should consider how an economy-wide governance framework in relation to data and digital technologies can ensure these laws work together effectively in a fast-changing environment.[76] Embracing such integrated governance frameworks is recognised as being key to delivering the societal outcomes desired from a data-driven, highly-digitised economy.[77] Consumers protections that are fit for a modern, highly digitised economy will also be essential to the post-COVID-19 economic recovery of Australia over the coming years.

Consistent, coherent and quality governance framework across a range of institutions, organisations and markets will help to support innovation and economic growth – and ensure that the various laws and regulations that protect consumers can adapt and keep pace with change.[78] The government's own Digital Economy Strategy recognises how the rapid pace of data driven technological advances throws up challenges in respect to laws and regulation.[79] Developing an economy-wide governance framework will help with tackling such challenges by ensuring all relevant laws and regulations:

- Are more closely linked to the needs of citizens and businesses,
- Adapt faster to change,
- Minimise negative impacts on innovation, and
- Ensure maximum access to international markets.

Given the current federal government's ambitions for Australia to be a world leading digital economy by 2030, it is essential for there to be a clear strategy for how integrated consumer protections work together in future to foster a fair, safe and inclusive digital economy for consumers and businesses. The Australian economy will become increasingly digitised and technology will continue to evolve, regardless of the policy and regulatory interventions the government makes. What such government interventions will dictate is the extent to which these trends benefit Australian consumers and society overall.

CPRC has highlighted in previous submissions to government the significant risks to the community and economy of an ongoing fragmented and piecemeal policy framework.[80] At the moment the development of the Privacy Act reforms appear to be siloed, with little detail in the Issues Paper as to how other economy-wide reforms should interact (such as the

---

[74] Office of the Victorian Information Commissioner, "To consent and beyond: are No-Go Zones the next frontier? – Part 2", (January 2020), https://ovic.vic.gov.au/blog/to-consent-and-beyond-are-no-go-zones-the-next-frontier-part-2/

[75] Refer to Question 67.

[76] The World Economic Reform stresses the importance of "agile governance" frameworks in the context of the Fourth Industrial Revolution. Such governance ensures that government policies are "generated, deliberated, enacted and enforced" in a way that can keep pace with the rapid changes emerging technology is causing within society. See: Klaus Schwab, "The Fourth Industrial Revolution: what it means, how to respond", (January 2016), https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ ; and World Economic Forum, "Agile Governance – Reimagining policy-making in the Fourth Industrial Revolution", (January 2018), 6-7, http://www3.weforum.org/docs/WEF_Agile_Governance_Reimagining_Policy-making_4IR_report.pdf

[77] Shinzo Abe, "'Defeatism about Japan is now defeated': Abe's Davos speech in full", (January 2019), https://www.weforum.org/agenda/2019/01/abe-speech-transcript/

[78] Center for Strategic & International Studies, "Data Governance Principles for the Global Digital Economy", (June 2019), https://www.csis.org/analysis/data-governance-principles-global-digital-economy

[79] Australian Government, "Australia's Tech Future – Delivering a strong, safe and inclusive digital economy", (December 2018), 47, https://www.industry.gov.au/sites/default/files/2018-12/australias-tech-future.pdf

[80] CPRC, "Submission by Consumer Policy Research Centre to Australian Treasury consultation on the ACCC Digital Platforms Inquiry Final Report", (September 2019), 3-4.

Consumer Data Right (CDR), ACCC's recommendations to add unfair trading practices and unfair contract terms prohibitions into Australian Consumer Law[81]; reforms to competition laws to manage market power regarding data collection and use[82]; and the Australian Human Rights Commission's considerations of how to safeguard human rights in the context of data and technology[83]).

We also note and support the point made in the FRLC, CALC and FCA joint submission to this Review on the need to harmonise the Privacy Act with the CDR, particularly in relation to the lack of protections for consumers when data is accessed by non-accredited CDR parties. Given the intention for the CDR to become an economy-wide data access and sharing scheme – opening up more consumer data across the economy over the coming years – this reform must also be coupled with adequate economy-wide Privacy Act and Australian Consumer Law protections so that industry is incentivised to participate in this more effective and trusted data collection and sharing scheme, as compared with current practices which expose consumers to unacceptable harms such as screen scraping. Australia's governance and protection framework must encourage safe, fair and trusted innovation and competition, rather than incentivise "a race to the bottom" regarding the quality of data-driven products and services received by consumers.

FURTHER ENGAGEMENT

CPRC looks forward to continuing to engage with the Attorney-General's Department over the coming weeks and months as reforms to the Privacy Act take shape. We are encouraged by the breadth of issues currently considered for reform – and reiterate our message that government seize this reform opportunity by making bold improvements to the privacy protections afforded to Australian consumers. It is essential that our privacy protections – and protections regarding consumer law, human rights and competition – keep pace with both technological change and international regulatory developments if Australia is to become a world-leading digital economy by 2030.

For further discussions regarding our upcoming research and the contents of this submission, please contact Andrew Thomsen, Senior Research and Policy Manager (andrew.thomsen@cprc.org.au) or Emma O'Neill, Research and Policy Director (emma.oneill@cprc.org.au).

Lauren Solomon
Chief Executive Officer
Consumer Policy Research Centre

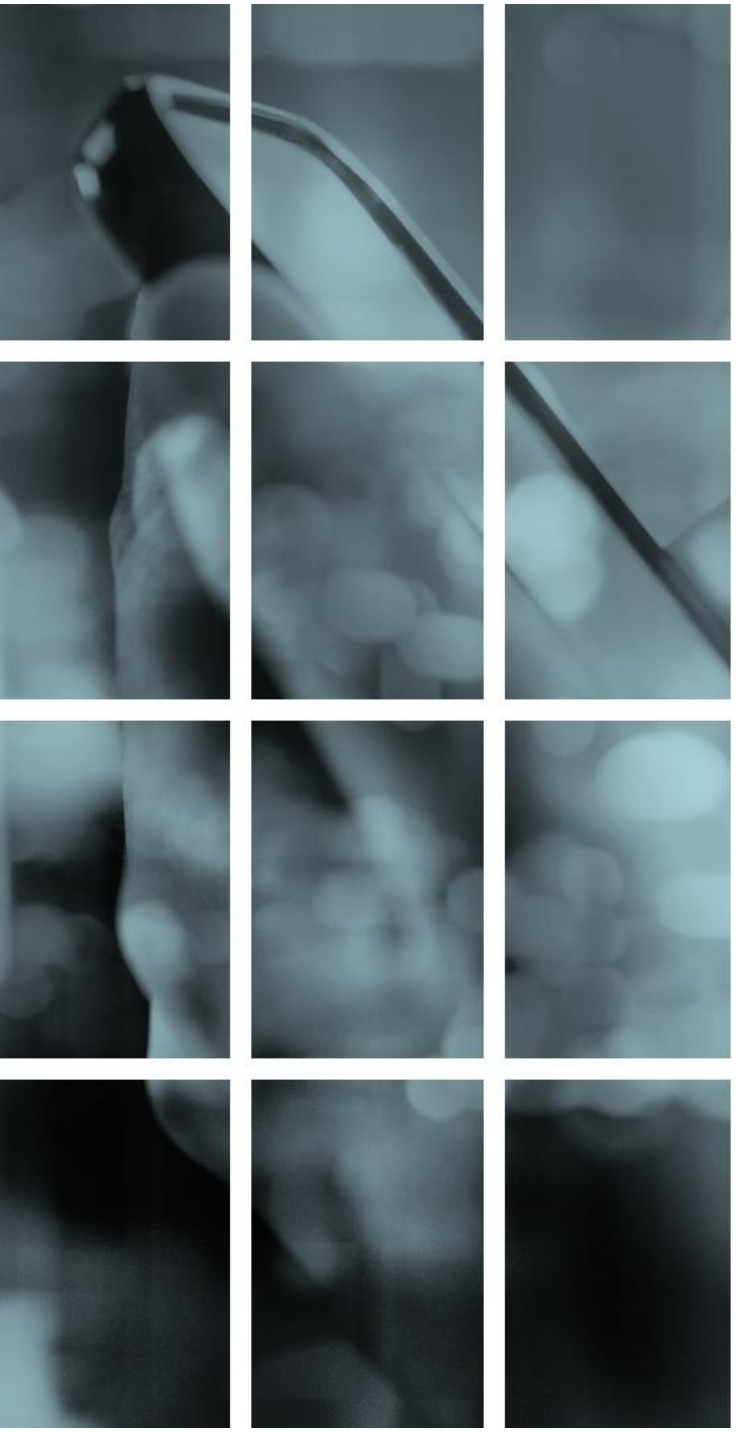
[81] See recommendations 20 and 21 in: ACCC, "Digital Platforms Inquiry – Final Report", (June 2019).
[82] See recommendations 1 and 2 in: Ibid.
[83] AHRC, "Human Rights and Technology – Discussion Paper", (December 2019), 189-193.

CPRC 2020 Data and Technology Consumer Survey

Consumer research conducted in partnership with Roy Morgan Research over March and April 2020

Consumer Policy Research Centre

Contents



Executive Summary

Overview of our consumer research findings

CPRC's 2020 Data and Technology Consumer Survey reveals the increasing reliance consumers have on digital technologies, products and services.

- 70% of Australians use Google products or services daily, while 58% use Facebook daily.
- 28% of 2020 survey respondents visited online shopping websites at least once a week, up from 21% in 2018.
- Location apps and GPS devices were by far the most commonly used internet-connected devices (69% of consumers) – while smart assistants (32%) and exercise health trackers (24%) were also commonly used.

Privacy Policies offer no protection when the majority of consumers don't read them. Australians also view the sharing and selling of personal information by companies as an unfair practice.

- Privacy Policies and Terms and Conditions (T&Cs) continue to be ineffective at informing consumers of company data-handling practices – 94% of Australians are not reading this information all the time.
- Of consumers who had read a Privacy Policy or T&Cs in the past 12 months, 69% admitted to having agreed to them for at least a few products/services despite feeling uncomfortable doing so.
- 85% of consumers consider it is unfair for companies to share personal information they've provided with other companies – while 90% think it is unfair for this information to be sold to other companies. A large majority of consumers also find it unfair when companies collect more information than is necessary to deliver the product or service they are receiving (88%).
- Consumers have high concerns about online safety issues, with concern highest regarding data breaches or hacks (94%), personal data being used for fraud or scams (93%) and children's data being misused (92%).

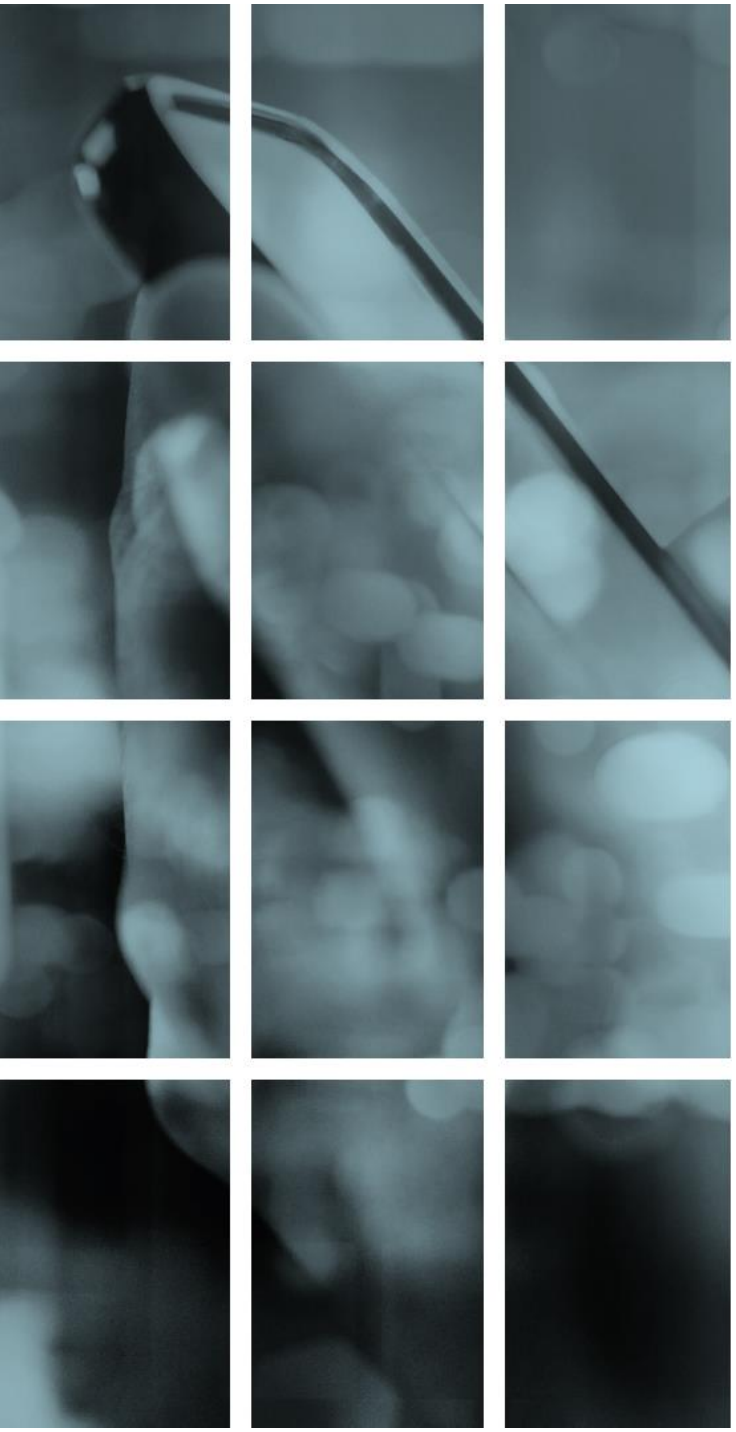
Overview of our consumer policy insights

Consumers consider that both companies and government have high levels of responsibility for making sure consumers are protected from unfair and harmful data practices.

- A majority of Australians consider companies have a “high” level of responsibility in protecting their personal information, for example:
    - protecting against consumers’ information from being used in ways that make them worse off (82%)
    - protecting consumers against collection and sharing of their personal information (75%).
- Government is also seen to have high responsibilities in these areas (79% and 67% respectively) – while 80% of consumers consider government has a “high” level of responsibility for developing protections to ensure no one is excluded from essential products or services based on their data.

Market and regulatory failures in relation to companies’ data-handling practices mean that digital marketplaces are failing to deliver fair outcomes to consumers.

- At a time when COVID-19 has increased consumer reliance on digital technologies and marketplaces, Australians are left to rely on analogue laws and regulations to protect them in an increasingly digital world.
- Australia’s consumer protections need to be modernised so that consumers are protected against practices that unfairly exploit information asymmetries, bargaining power imbalances and behavioural biases in digital marketplaces.
- Reform processes already announced – such as an unfair trading practice prohibition and general safety provision being added to Australian Consumer Law, and a comprehensive review of the Privacy Act – need to deliver stronger protections without delay. This will ensure Australian consumers are properly protected, and help to drive greater trust and confidence in digital marketplaces, as the economy recovers from COVID-19.



Introduction to our research

Background

The Consumer Policy Research Centre (CPRC) is an independent, not-for-profit organisation that undertakes interdisciplinary and cross-sectoral consumer research. We want markets to deliver a fairer, safer and more inclusive future for consumers.

Data and technology issues are a research focus for CPRC, including emerging consumer risks and harms and the opportunities to better use data to improve consumer wellbeing and welfare.

In 2018, CPRC engaged Roy Morgan Research (Roy Morgan) to conduct a survey regarding Australians' knowledge, behaviours and attitudes regarding data collection, sharing and use. In 2020 Roy Morgan were engaged to refresh the survey findings from 2018 – and also expand the research scope to cover recent developments in data technology, collection, sharing and use.

This report presents the findings of the 2020 survey – drawing out some key consumer policy insights from the results. The research builds off extensive research from CPRC relating to data, digital marketplaces and the outcomes consumer both experience and expect. This past research includes:

- ***Data and the Digital Economy*** report in 2018
- ***The Day in the Life of Data*** report in 2019
- ***Consumers and COVID-19: from crisis to recovery*** report in 2020.

Research objectives and methodology

The objectives of our consumer research was to build on our understanding of Australians' behaviours and attitudes towards digital marketplaces, in terms of:

- interactions with different data-driven products and services
- knowledge and acceptance of data collection, use and sharing
- attitudes towards the use of data for marketing and personalised pricing
- concerns towards personal data breaches and misuse
- responsibilities of consumers, government and companies with regard to protection.

To fulfil these objectives, a nationally representative online survey of 1000 consumers aged 18 or over was undertaken between 19 March and 1 April 2020, in partnership with Roy Morgan. The survey results have been weighted so they are representative of the Australian population.

The online survey was supplemented by in-depth 30 minute telephone interviews of 10 online survey respondents carried out between 6-8 April 2020. A selection of quotes from these interviews are included throughout the report.

How to read this report

This report is divided into four parts - reflecting the focus of our consumer research.

Part one is about the reliance Australian consumers have on data-driven technologies and "***digital marketplaces***"* – and explores how this reliance has evolved since 2018. It looks at what technologies, products and services Australians are using and what this means for their daily lives.

Note: *our consumer survey took place mostly in March 2020 – before COVID-19 restrictions fully set in. On p. 15 we highlight other research that shows how consumer behaviours have changed dramatically due to COVID-19 restrictions.*

Part two is about current consumer attitudes toward data practices and privacy – and how these compare to our 2018 survey results.

Part three explores consumer attitudes toward fairness, safety and responsibility for protections in digital marketplaces. All of these questions were asked for the first time in our 2020 survey.

Part four sets out the key consumer policy implications our research results pose – and what can be done by market stewards to ensure consumers interests are promoted in digital marketplaces.

CPRC uses the term "digital marketplaces**" to mean a broad range of online locations – for example, apps, websites or digital platforms – where consumers can engage in activities such as accessing and receiving information, comparing propositions and finalising transactions (be they monetary or data-based).*

Part One

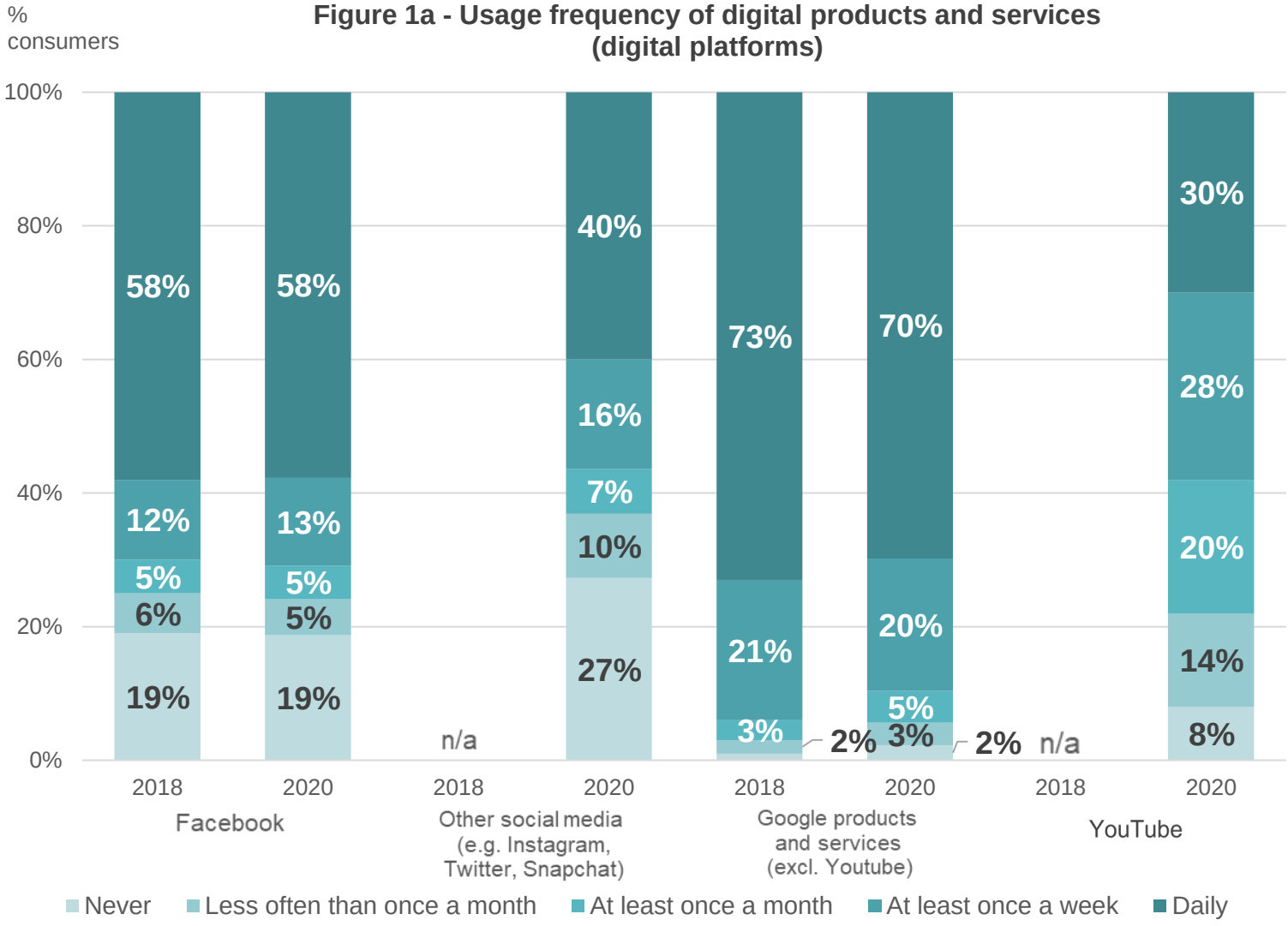
Consumer usage and reliance on data-driven products and services

Consumers continue to use digital platforms at a high frequency – with over half of consumers using Google and Facebook products daily

Use of Google products and services remained stable between 2018 and 2020, with 70% of consumers continuing to use these daily. 58% of Australians also used YouTube at least once a week.

Social media was commonly used, with 58% and 40% of Australians being daily users of Facebook and “Other social media” respectively.

Figure 1a - Usage frequency of digital products and services (digital platforms)



Q: In the past 12 months how often did you use:

***Note** – data labels ≤ 1% are not shown*

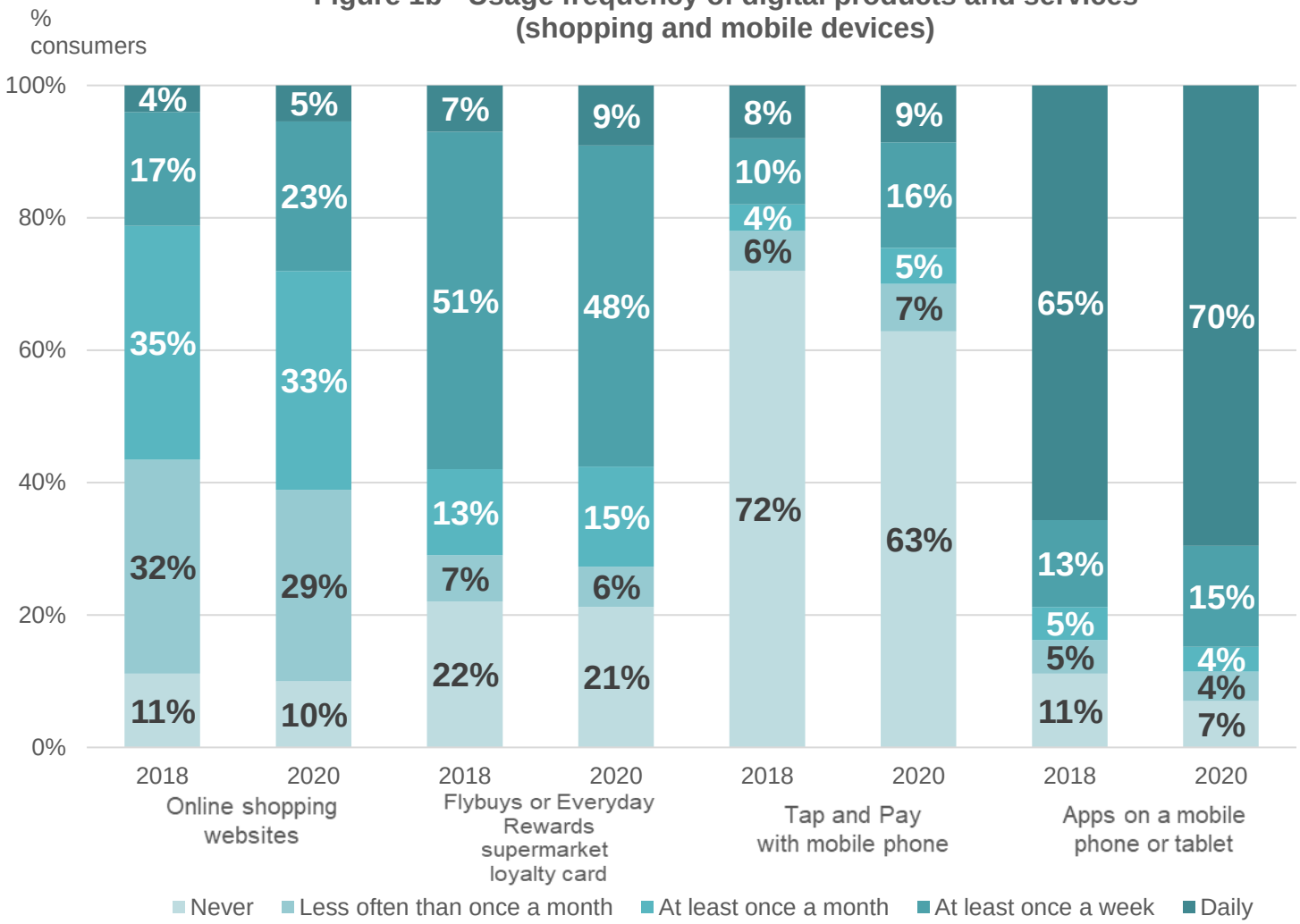
There were significant increases regarding usage of apps and online shopping between 2018 and 2020

28% of 2020 respondents visited online shopping websites at least once a week, well up from 21% in 2018.

There were also significantly more daily users of apps on mobile phones or tablets in 2020 (70%) compared to 2018 (65%).

Tap and Pay use also increased - with 25% of consumers using this technology at least once a week (18% in 2018).

Figure 1b - Usage frequency of digital products and services (shopping and mobile devices)



Q: In the past 12 months how often did you use:

Our survey indicates that 81% Australians are currently using internet connected devices

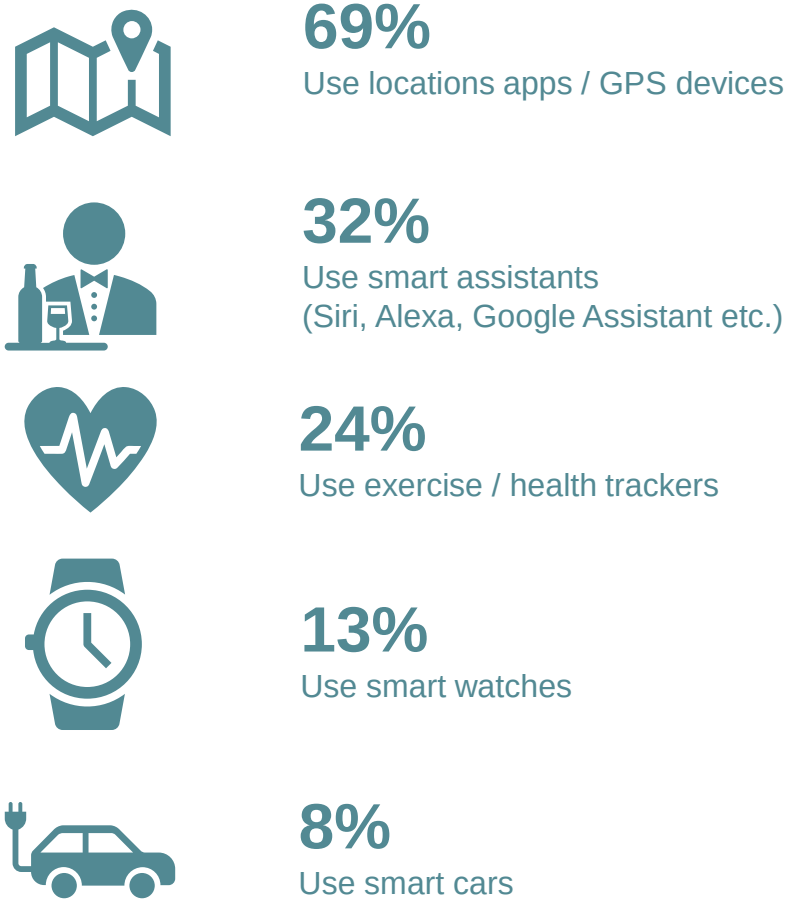
Locations apps and GPS devices were the most commonly used internet-connected device (69%), followed by smart assistants (32%) and exercise health trackers (24%).

The survey also revealed that less than 8% of Australians currently use the following internet connected devices:

- Smart household appliances (7%)
- Smart home security system (6%)
- Smart thermostat (2%)
- Smart baby monitor (2%).

19% of consumers indicated that they did not use any of the internet connected devices we asked about.

Figure 2 - Internet connected devices consumers are using



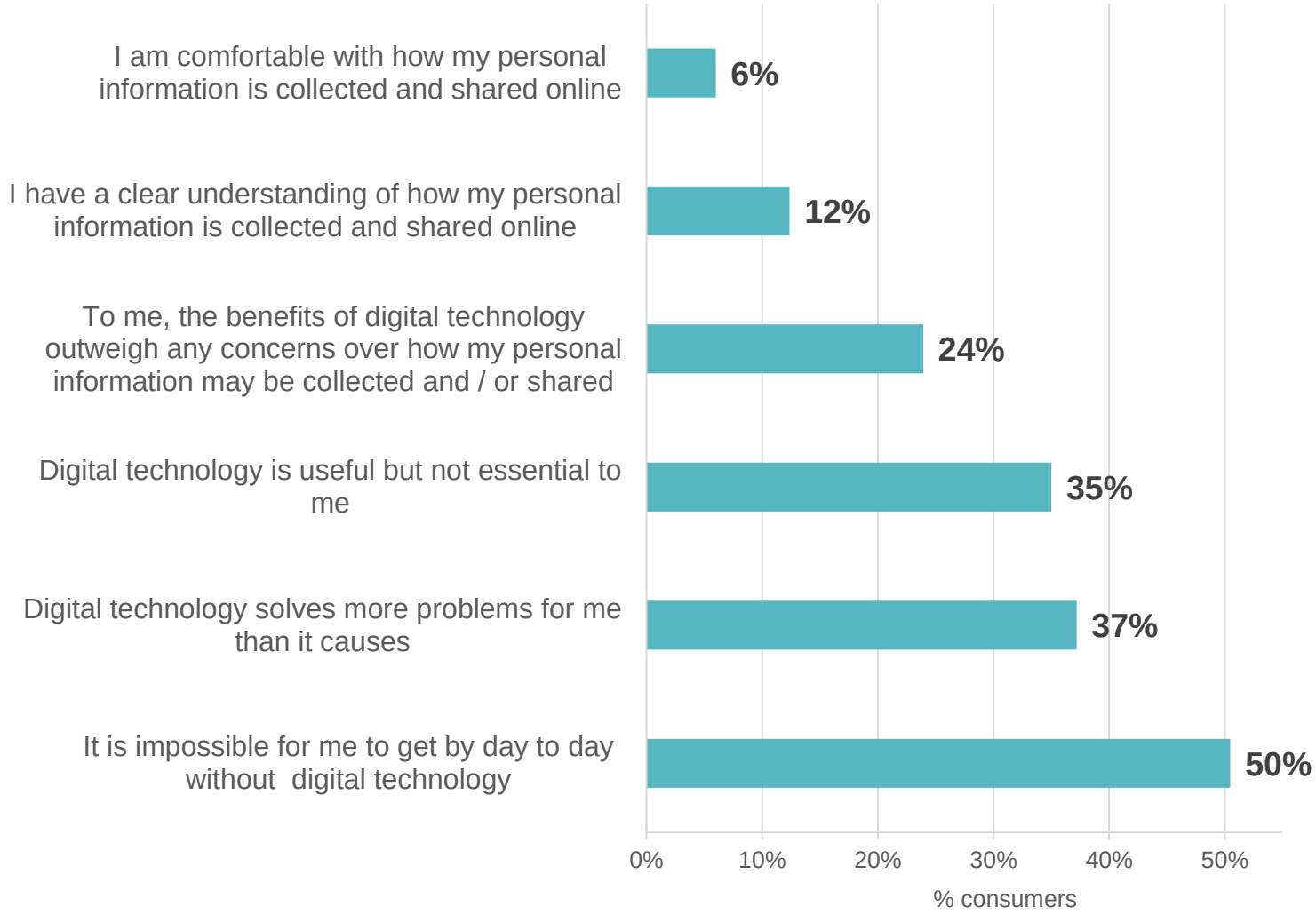
Q: Which of the following internet connected devices do you currently use:

While there is a heavy reliance on digital technology among many Australians, most do not feel comfortable or properly informed with how their personal information is handled online

Only 12% of consumers feel that they have a clear understanding on how their personal information is collected and shared.

Only 6% of consumers are comfortable with how their personal information is collected and shared online.

Figure 3 - Consumer attitudes towards digital technology



Q: Which of the following statements do you agree with:

Due to COVID-19, consumption of digital products and services has exploded in recent months

Consumer research from other organisations – conducted after CPRC's survey – shows how consumer behaviours have changed dramatically due to COVID-19.

- ***eSafety Commissioner*** research shows how people have been using the internet "a lot more" for staying up to date with news (30%), work (27%), watching videos (27%), and social media (25%). 10% of respondents reported shopping online "a lot more."
- ***Office of the Australian Information Commissioner*** research shows that 47% of Australians have downloaded an app or signed up to a new digital service due to COVID-19.
- ***Australian Communications and Media Authority*** research found that in the first six months of 2020 more Australians had participated in a range of online activities compared to 2019, with the biggest jumps seen relating to watching videos (83% 2019, 89% 2020) and shopping (78% 2019 to 83% 2020) online.

Figure 4 – Respondent quotes about the impact of COVID-19 restrictions on how often they are online

"My classes are now online, so I spend even more time on the internet."

"Now that I'm working from home; I seem to spend every moment online."

"I already spent most of my time online."

Q: (As of early April 2020) do you find that in the last few weeks (with everything that's going on), you have been using the internet more than usual, about the same amount or actually less than before?

Part Two

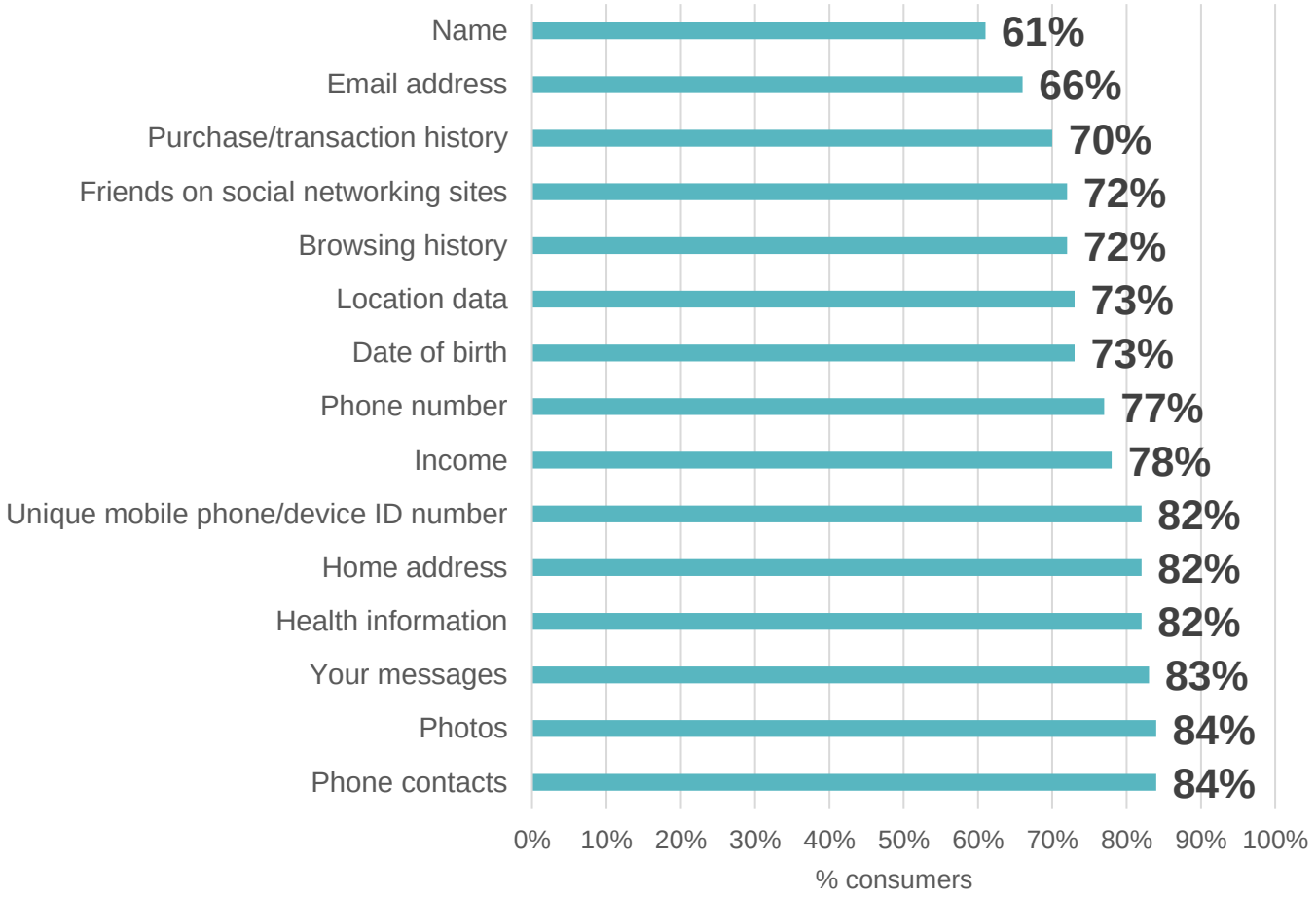
Consumer attitudes toward data handling and privacy practices

More than 60% of Australians were uncomfortable with companies sharing their personal information with third parties for purposes other than delivering products and services they'd signed up for

Over 8 out of 10 consumers are uncomfortable with the unnecessary sharing of information regarding their:

- phone contacts (84% 2020, 87% 2018),
- photos (84% 2020, n/a 2018)
- messages (83% 2020, 86% 2018)
- unique ID numbers for mobile phone/devices (82% 2020, 84% 2018).
- Health information (82% 2020, n/a 2018)
- Home address (82% 2020, n/a 2018).

Figure 5 - Information consumers are uncomfortable with companies sharing with third parties for purposes other than delivering a product or service



Q: What data/information would you be uncomfortable with companies sharing with third parties for purposes other than delivering the product or service?

Privacy Policies and T&Cs continue to be ineffective at engaging Australians – 94% of consumers are not reading this information all the time

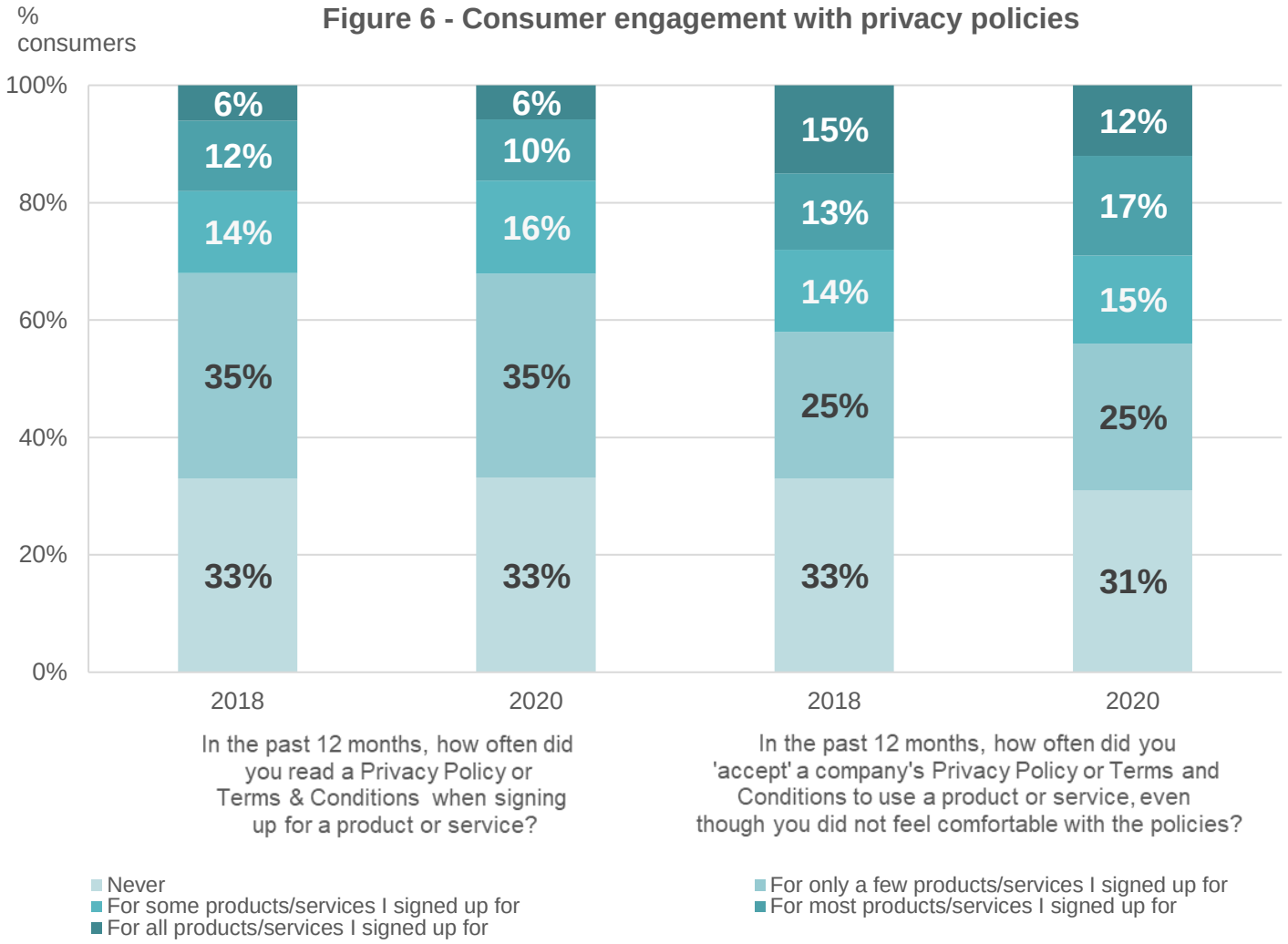
Reading of Privacy Policies and T&Cs did not change between 2018 and 2020. 33% of consumers never read these documents, and 35% read them only for a few products/services.

"Hardly anyone reads the Terms and Conditions and it's so long and detailed, you can't really get the critical data from it."

"It's really quite hard to find the Terms and Conditions, then they are generally not written to provide information easily."

Of the 67% of 2020 survey respondents who said they had read Privacy Policies or T&Cs in the past 12 months - 69% reported accepting terms even though they were not comfortable with them.

Figure 6 - Consumer engagement with privacy policies

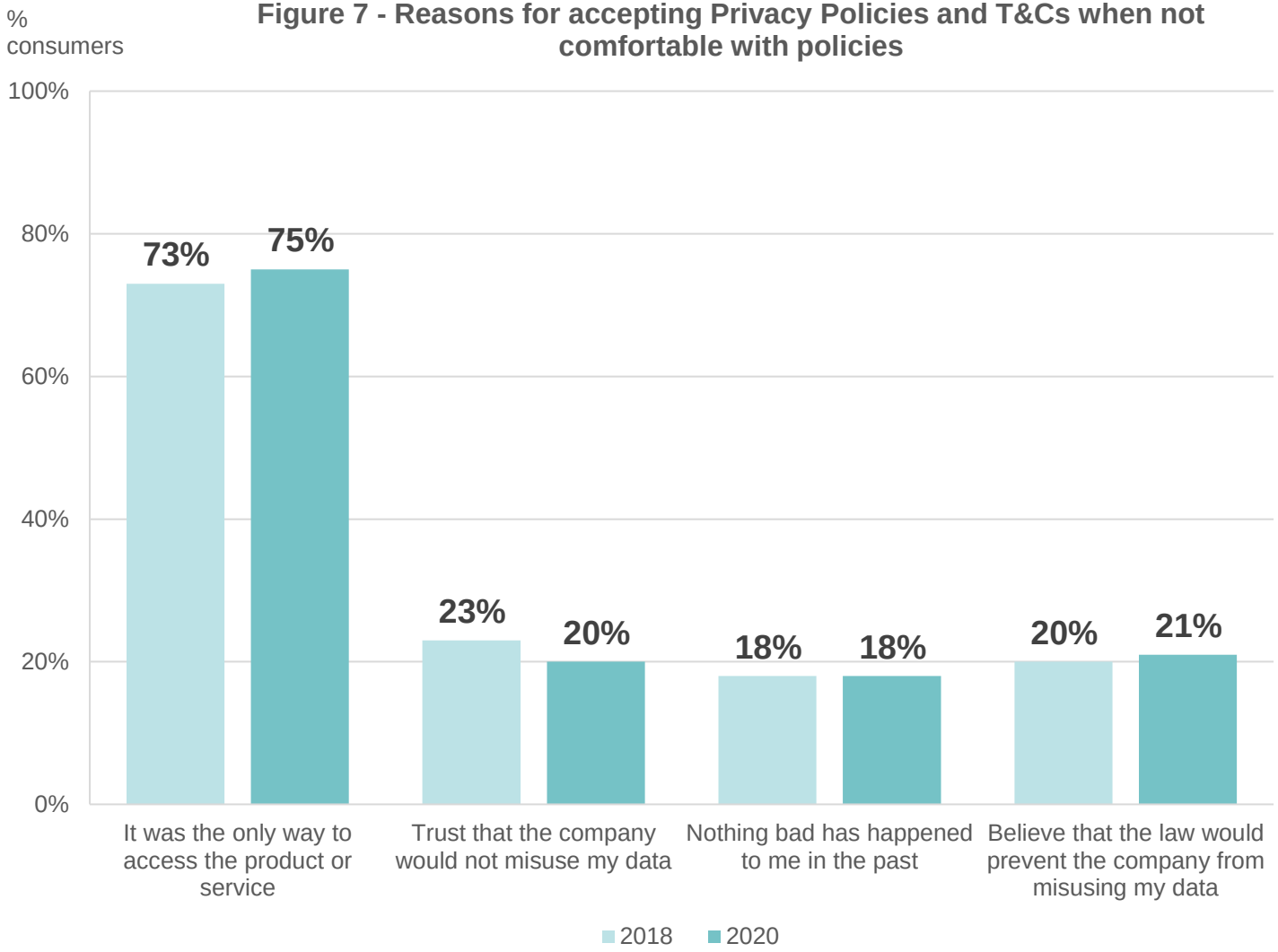


Of the Australians who had felt uncomfortable accepting Privacy Policies and T&Cs in the past 12 months, 75% did this because “it was the only way to access the product or service”

20% of consumers accepted Privacy Policies and T&Cs because they trusted the company would not misuse their data.

21% of consumers accepted - believing that the law would prevent the company from misusing their data.

Figure 7 - Reasons for accepting Privacy Policies and T&Cs when not comfortable with policies



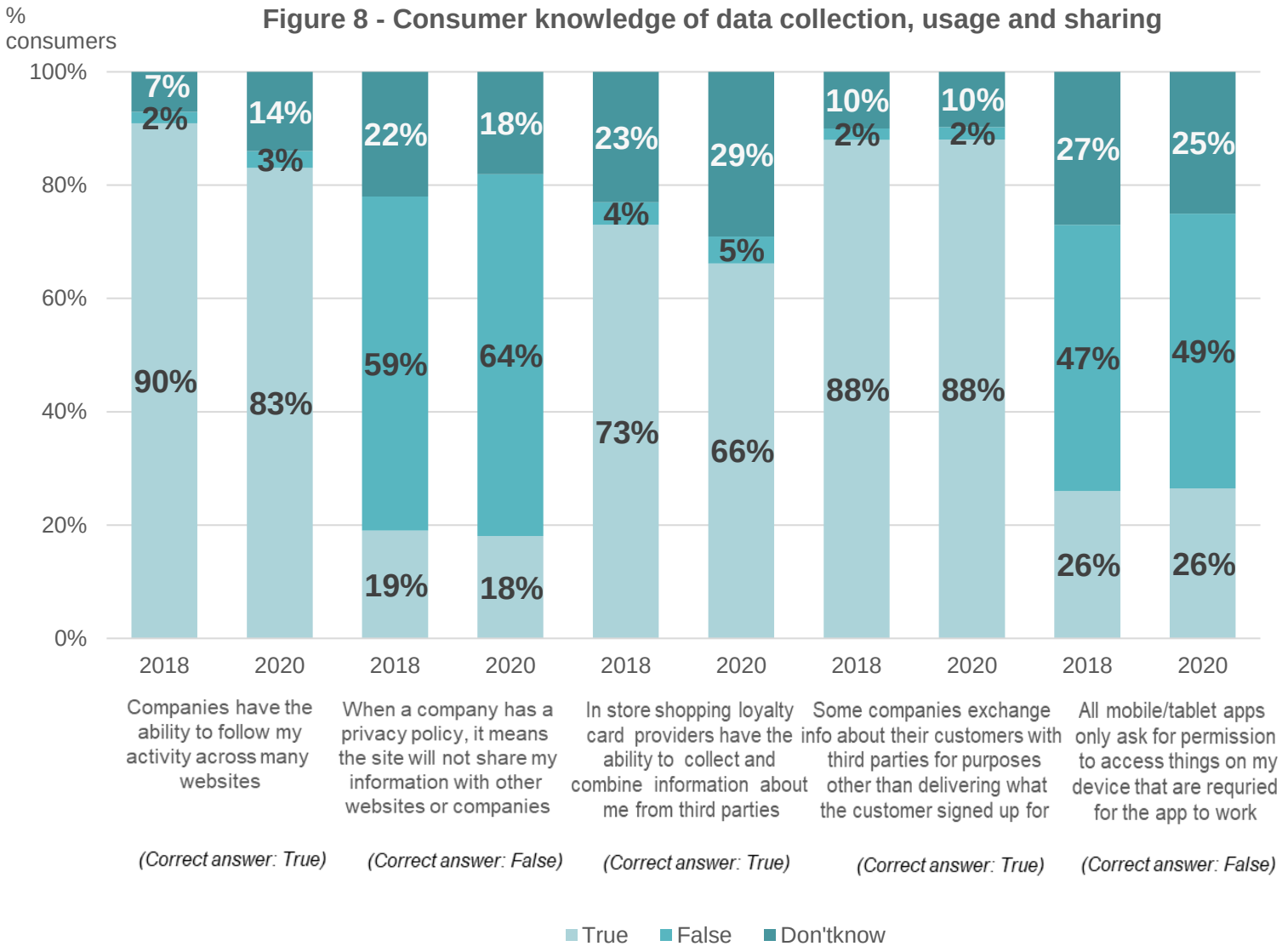
Q: Why did you 'accept' the Privacy Policy or Terms and Conditions even though you did not feel comfortable with the policies?

Since 2018 we have seen some drops in consumer knowledge concerning the data practices of companies they engage with

Less Australians are certain that companies today have the ability to follow their activities across many websites – with those knowing this to be true falling from 90% in 2018 to 83% in 2020.

The only significant increase in knowledge seen since 2018 was regarding a company having a Privacy Policy not meaning they won't share consumers' information with other websites or companies (59% knew this to be false in 2018; up to 64% 2020).

Figure 8 - Consumer knowledge of data collection, usage and sharing



Q: Choose True, False or Don't know for the following statements as best reflects your opinion:

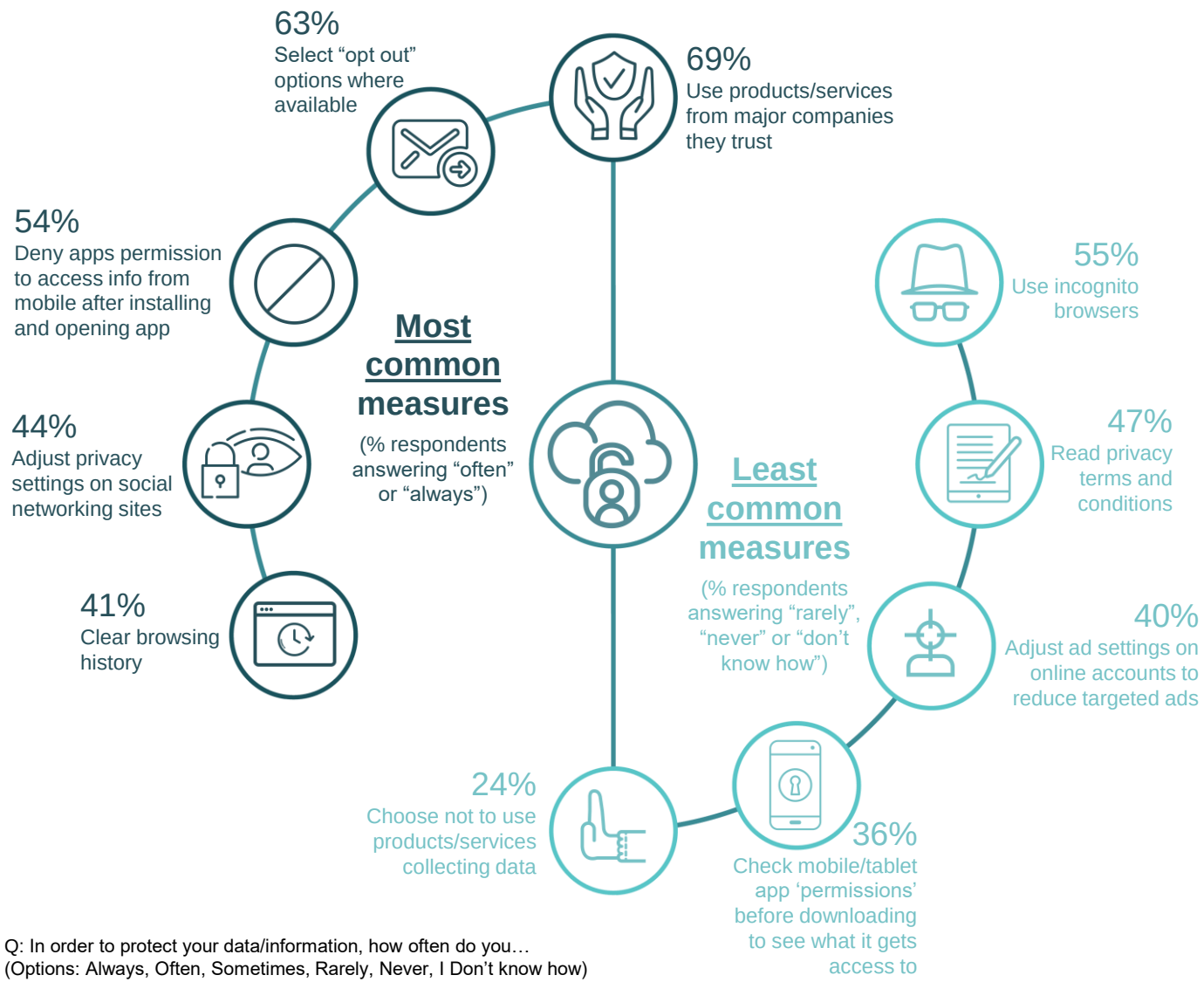
***Note** – totals may not add to 100% due to rounding*

“Opting out” of data being shared with third parties (when provided) is the most common measure “always” taken by consumers to protect their information – with 30% reporting they always do this.

The next most common measures “always” taken by consumers were to “deny apps permission to access information after install” and “adjust privacy settings on social networking sites” (both 21% “Always”).

Compared to the 2018 survey results, there was a significant increase in the number of Australians who “Never” clear their browsing history (5% in 2018, 8% in 2020); and significantly fewer Australians who “Always” check app ‘permissions’ before downloading (21% in 2018,17% in 2020).

Figure 9 – Summary of measures consumers take to protect personal information (2020 survey respondents)



Q: In order to protect your data/information, how often do you…
(Options: Always, Often, Sometimes, Rarely, Never, I Don’t know how)

Only 33% of consumers agree it's enough to be notified about data handling practices via Privacy Policies and T&Cs

A majority strongly agree or agree that companies should:

- Give options to opt out of certain types of information they can collect, use and share (95%)
- Be open about how personal data is used to assess eligibility or exclude them from products/services (94%)
- Only collect information needed for providing their products or services (92%).

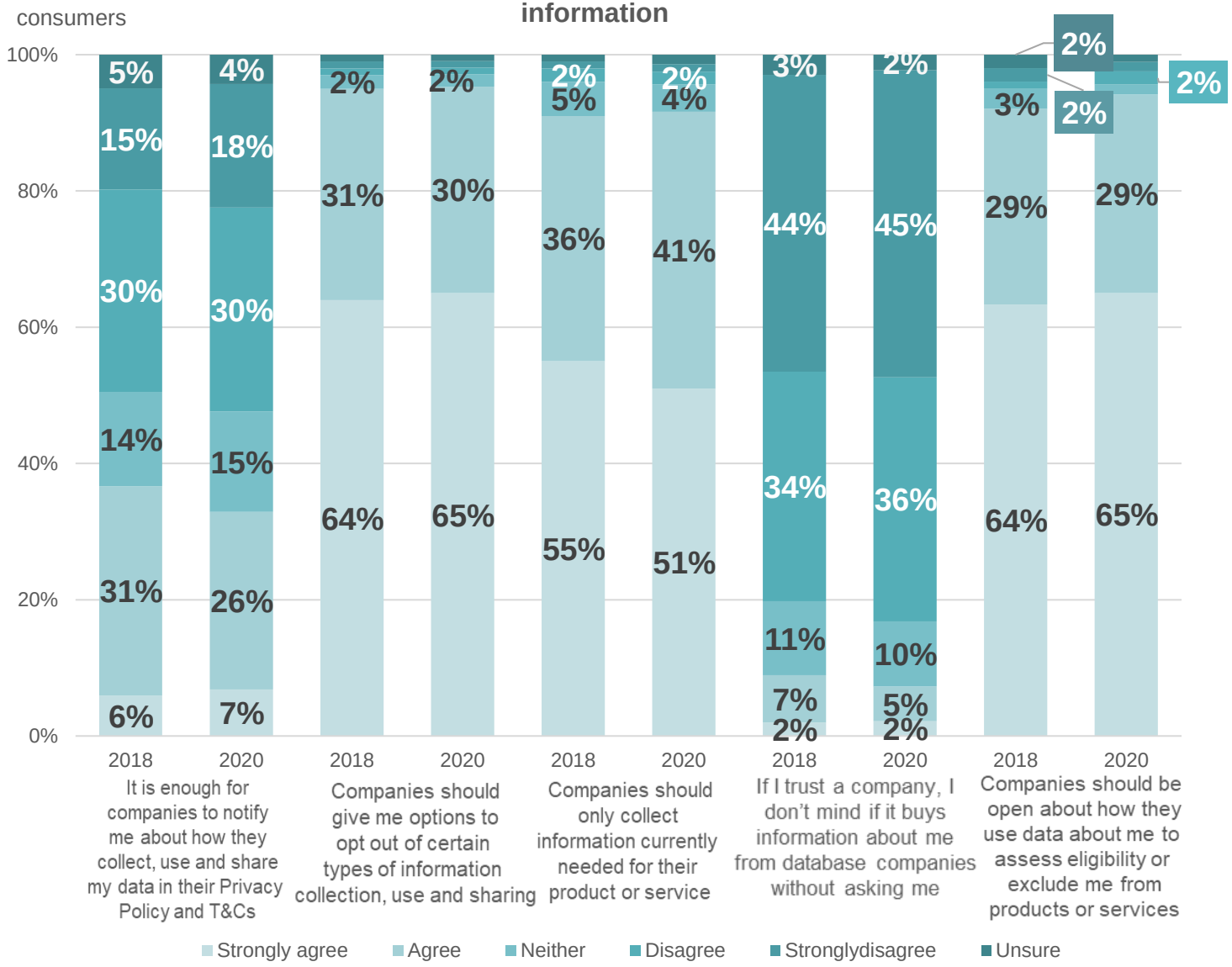
"I just think they have control of way too much... the person/ consumer can't do a thing about it."

92% consumers agree companies should only collect information they need for providing their product/ service

"They need to be more transparent about how this kind of information is being used."

94% consumers agree companies should be open how they use data about them (e.g. assessing eligibility or excluding consumers)

Figure 10 - Consumer expectations of companies' handling of personal information



Q: How strongly do you agree or disagree with the following regarding how companies should handle your data?

***Note** –data labels ≤ 1% are not shown*

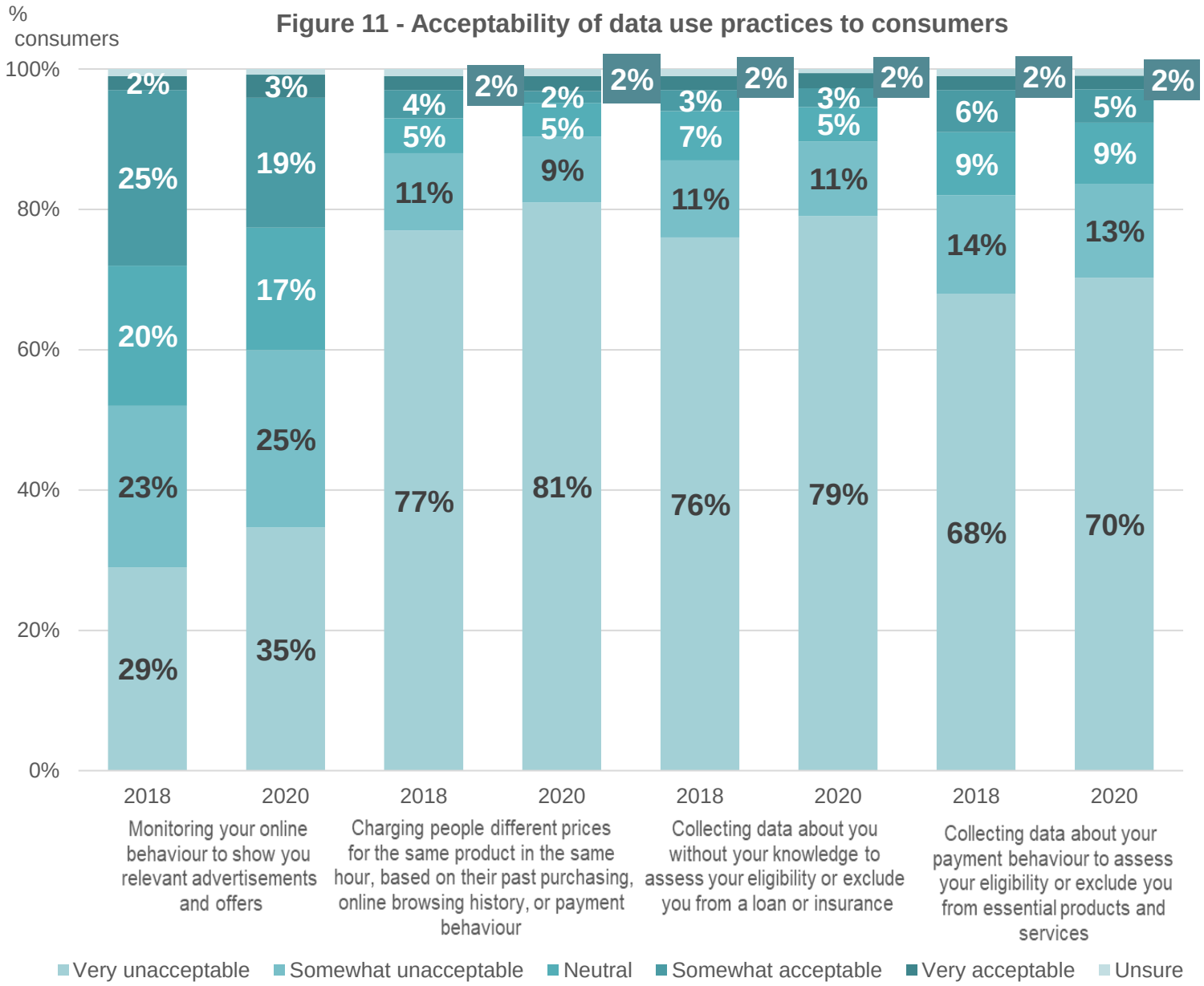
Opposition to ad targeting, personalised price discrimination and exclusion from products and services has increased since 2018

60% of Australians consider it very or somewhat unacceptable for their online behaviour to be monitored for targeted ads and offers – up from 52% in 2018.

90% of Australians rated the following practices as very or somewhat unacceptable:

- Charging people different prices based on past purchase, online browsing, and payment behaviours
- Collecting consumer data without their knowledge to assess their eligibility or exclude them from loans or insurance

Figure 11 - Acceptability of data use practices to consumers



Q: How acceptable or unacceptable do you find it for companies to use your data in the following ways?

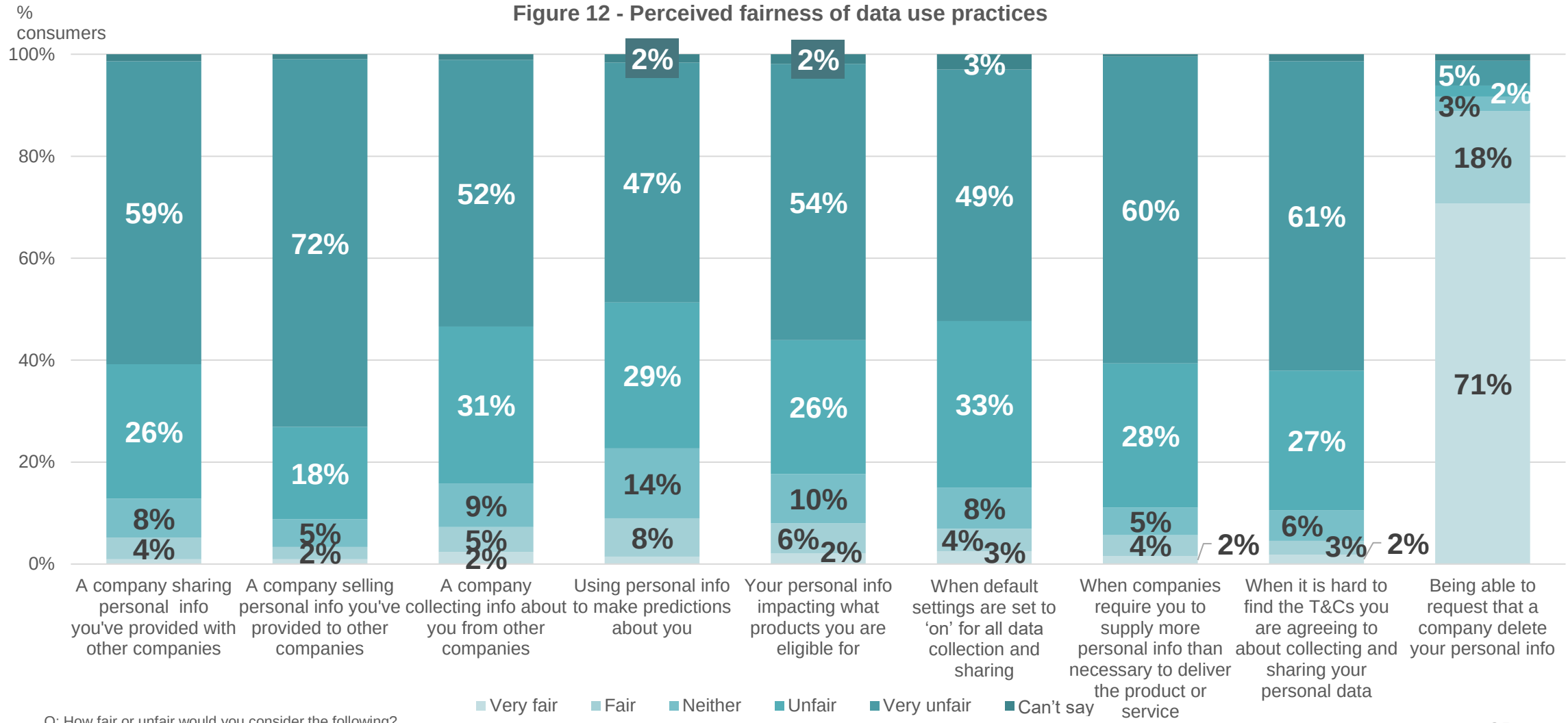
***Please note** – some data labels ≤ 1% are not shown*

Part Three

Consumer expectations of digital marketplaces

A large majority of Australians consider that the ways in which companies can collect, use and share their personal information is unfair

Figure 12 - Perceived fairness of data use practices



Q: How fair or unfair would you consider the following?

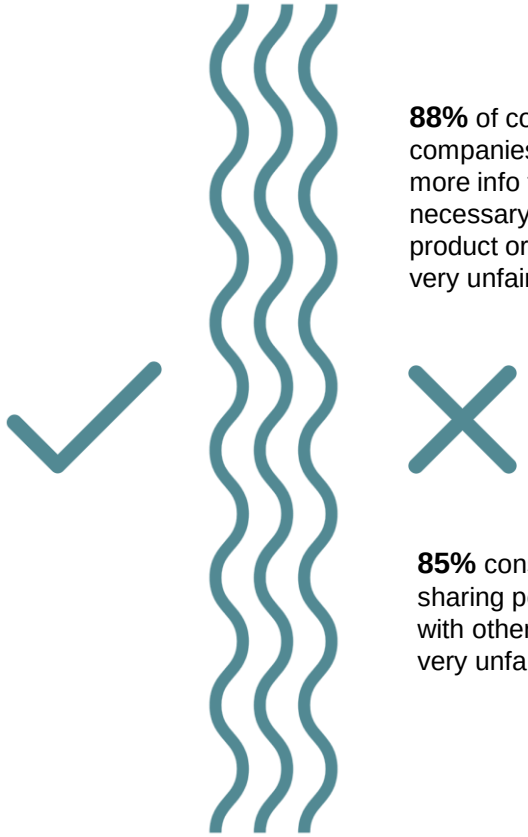
***Note** – data labels ≤ 1% are not shown*

Many data practices “cross a line” for consumers and are considered unacceptable

As shown in Figure 12 (p.25) a large majority of consumers consider many data handling practices to be either very unfair or unfair. These include companies:

- selling (90%) or sharing (85%) personal information they’ve provided to other companies
- requiring more personal information than is necessary to deliver a product or service (88%)
- collecting information about consumers from other companies (83%)
- using a consumer’s personal information to make predictions about them (76%)

Figure 13 – Consumers’ “line in the sand” regarding data handling practices



88% of consumers find companies requiring more info than is necessary for delivering a product or service to be very unfair or unfair

85% consumers find sharing personal info with other companies very unfair or unfair

“I think when you sign up for something, and you’re trusting them to not invade your personal privacy and take something that they don’t need from you.”

“Only getting the information strictly necessary for the current transaction and don’t share it with anyone.”

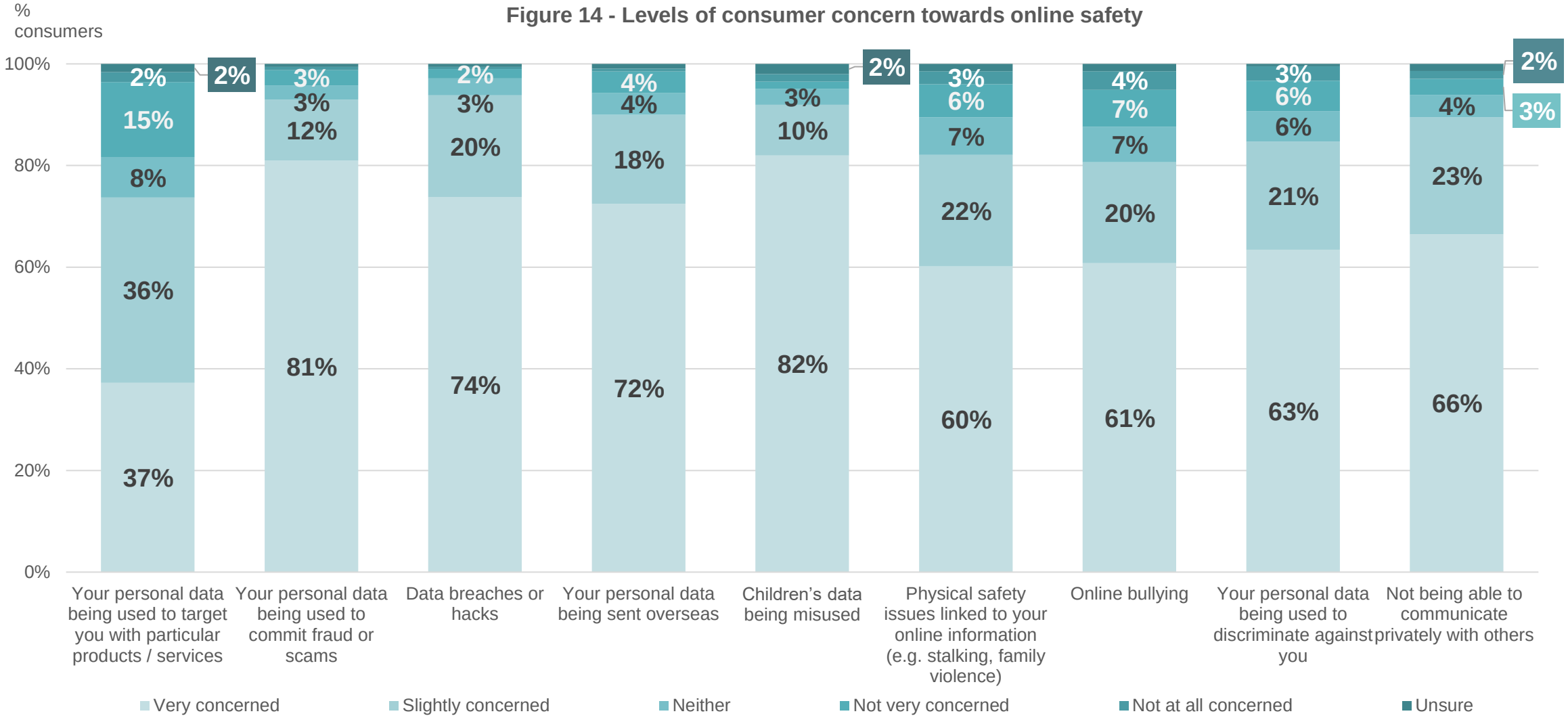
“I think sometimes it’s necessary for them to be collected (personal data), but sharing it, there’s no reason to.”

(My line in the sand is) once they share it.. They can collect it and store it for their own purposes, but it should stop there.”

Q: In your opinion, where is the line between acceptable and unacceptable behaviour of companies regarding personal data collection and sharing? Where do you draw your personal ‘line in the sand’?

Australians are greatly concerned with online safety in general – with a majority holding concerns regarding all the issues raised in the survey

Figure 14 - Levels of consumer concern towards online safety



Q: Thinking now about online safety, how do you feel about the following?

***Note** – data labels ≤ 1% are not shown*

Consumer concerns about online safety are highest regarding the safety of children, fraud and scams, data breaches and hacks; and personal data being sent overseas

Figure 14 (p. 27) shows how 9 out of 10 consumers were either very or slightly concerned about online safety regarding:

- Data breaches or hacks (94% of consumers)
- Personal data being used for fraud or scams (93%)
- Children's data being misused (92%)
- Personal data being sent overseas (90%)

Figure 15 – Consumer concerns regarding online safety

92% consumers very or slightly concerned about children's data being misused

"The risk to children is that they might give up too much information. They might have contact with unsafe people without the parents' knowledge"

89% consumers very or slightly concerned about not being able to communicate privately with others

"Why would you put a listening device in your own home? They say it's only active when you activate it, but the microphone is activated because the machine is listening. It activates at attention."

82% consumers very or slightly concerned about physical safety issues linked to online information

"There's probably some gender differences there, like if I were a female who had an ex-partner who was stalking, I would definitely feel unsafe (with location tracking). Like if someone were to track me because they were mad at me or something."

Q: There is a growing presence of children online (on social media, online purchases, using search engines). What risks, if any do you believe this presents to your safety and that of the children? (If risks mentioned) How did you learn about them?

Q: How about smart technologies / devices, such as Siri, Google Home, location apps, GPS devices, health trackers. What risks do you believe they present to your safety?

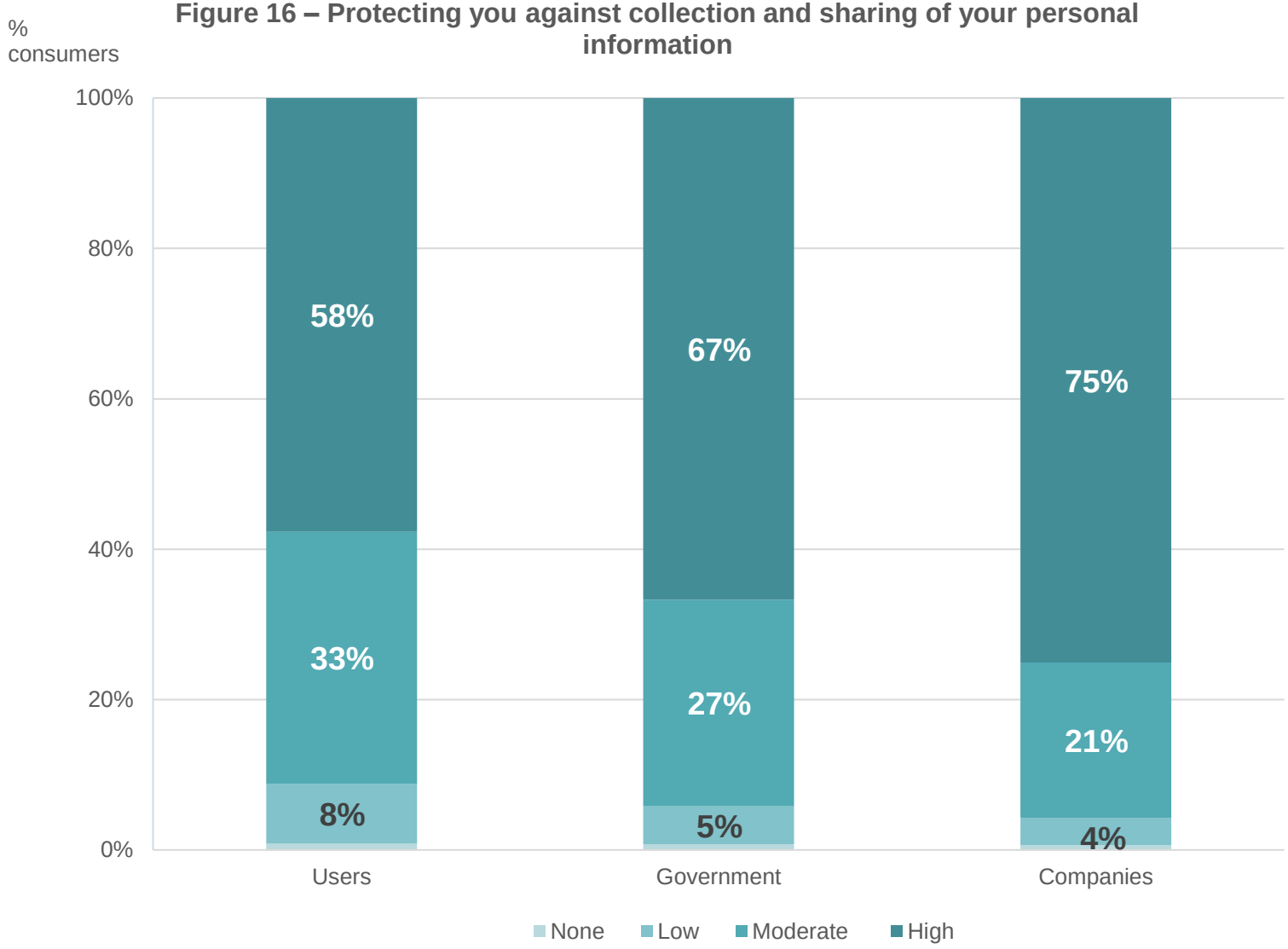
75% of consumers consider companies have the highest level of responsibility to provide protection against collection and sharing of personal information

67% of consumers also feel government has a high level of responsibility to protect consumers against collection and sharing of their personal information.

"I'd like to think the government (regulates it). Because with private competition, you just have so many different platforms, you can't just make rules for each platform, it has to be on a broader level."

67%
consumers think government has a high level of responsibility in protecting consumers

Figure 16 – Protecting you against collection and sharing of your personal information



Q: What level of responsibility do you think each of the following (Users/Government/Companies) should have in relation to:

***Note** – data labels ≤ 1% are not shown*

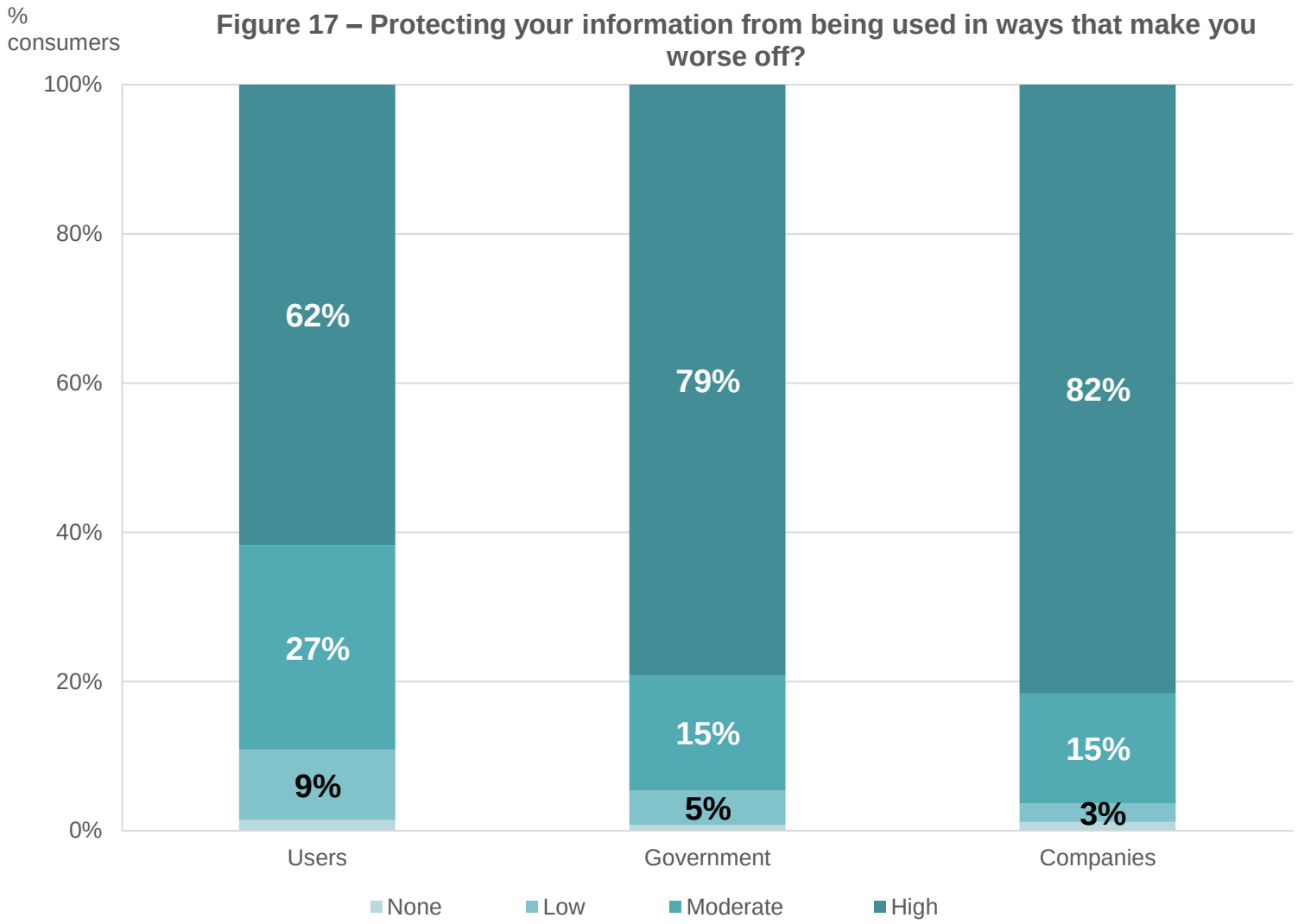
Consumers feel that both government (79%) and companies (82%) have high levels of responsibility to protect against personal information being used in ways that leave consumers worse off

Less consumers (62%), but still a majority, felt they had a high level of responsibility to protect themselves from being left worse off.

"Sometimes (targeted advertising) it can be unfair. I guess, (it) depends what you're clicking into. Especially with things like Cash Converters and Wallet Wizard and those sorts of things directed towards low socioeconomic households, stuff like that. That's dangerous, if you don't know what to press."

79% consumers think government have a high level of responsibility to ensure personal information is not used to make consumers worse off

Figure 17 – Protecting your information from being used in ways that make you worse off?



Q: What level of responsibility do you think each of the following (Users/Government/Companies) should have in relation to:

***Note** – data labels ≤ 1% are not shown*

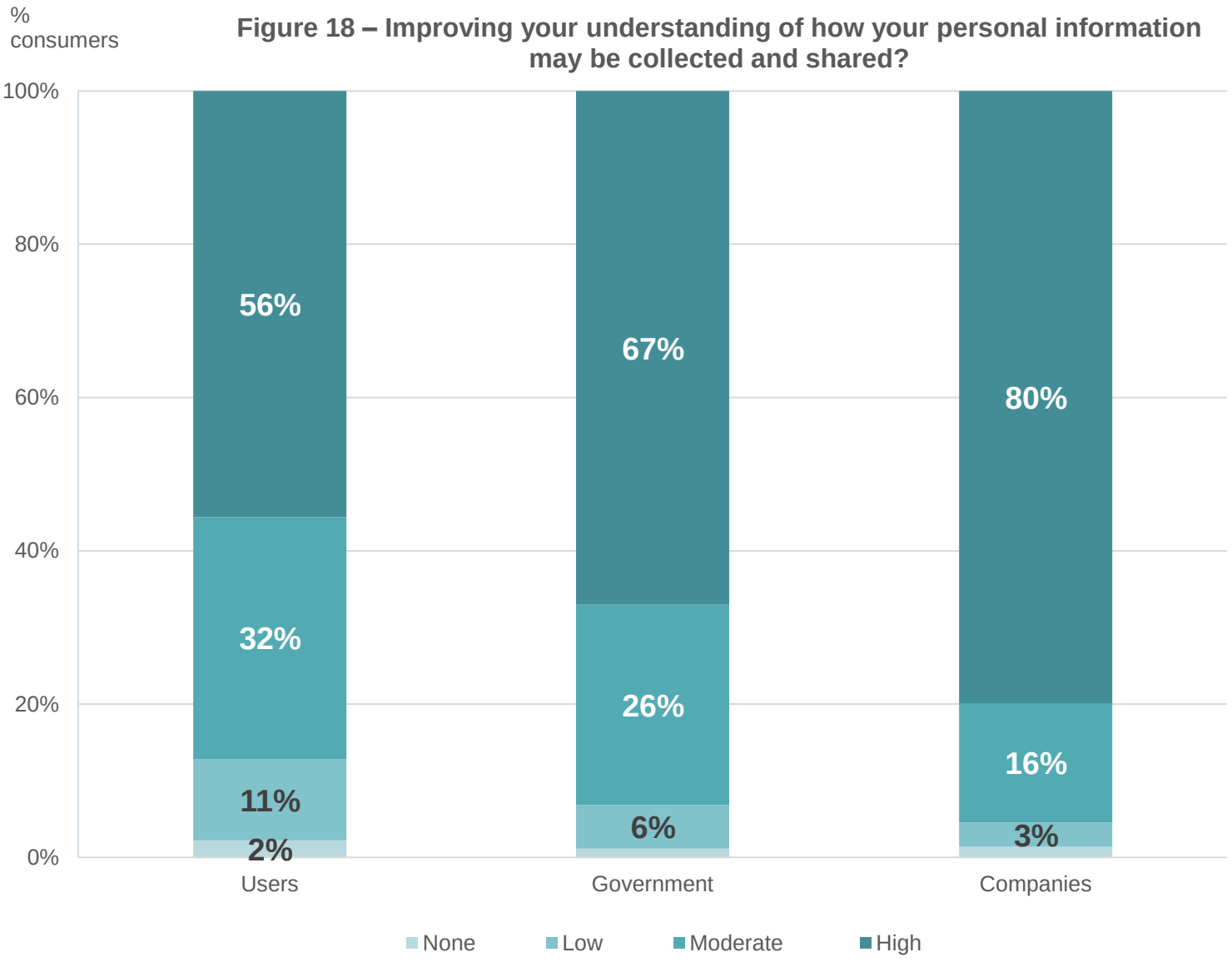
80% of consumers feel companies have a high level of responsibility to improve consumer understanding of personal information collection and sharing practices.

A large majority of consumers also felt government (67%) had high responsibility to improve consumer understanding of these practices.

"If you're searching a company and going on to their website, and to get information, you have to put in your details, it's your choice then you want to do it or not."

56% consumers think they have a high level of responsibility to improve their understanding of how their information is collected and shared

Figure 18 – Improving your understanding of how your personal information may be collected and shared?



Q: What level of responsibility do you think each of the following (Users/Government/Companies) should have in relation to:

***Note** – data labels ≤ 1% are not shown*

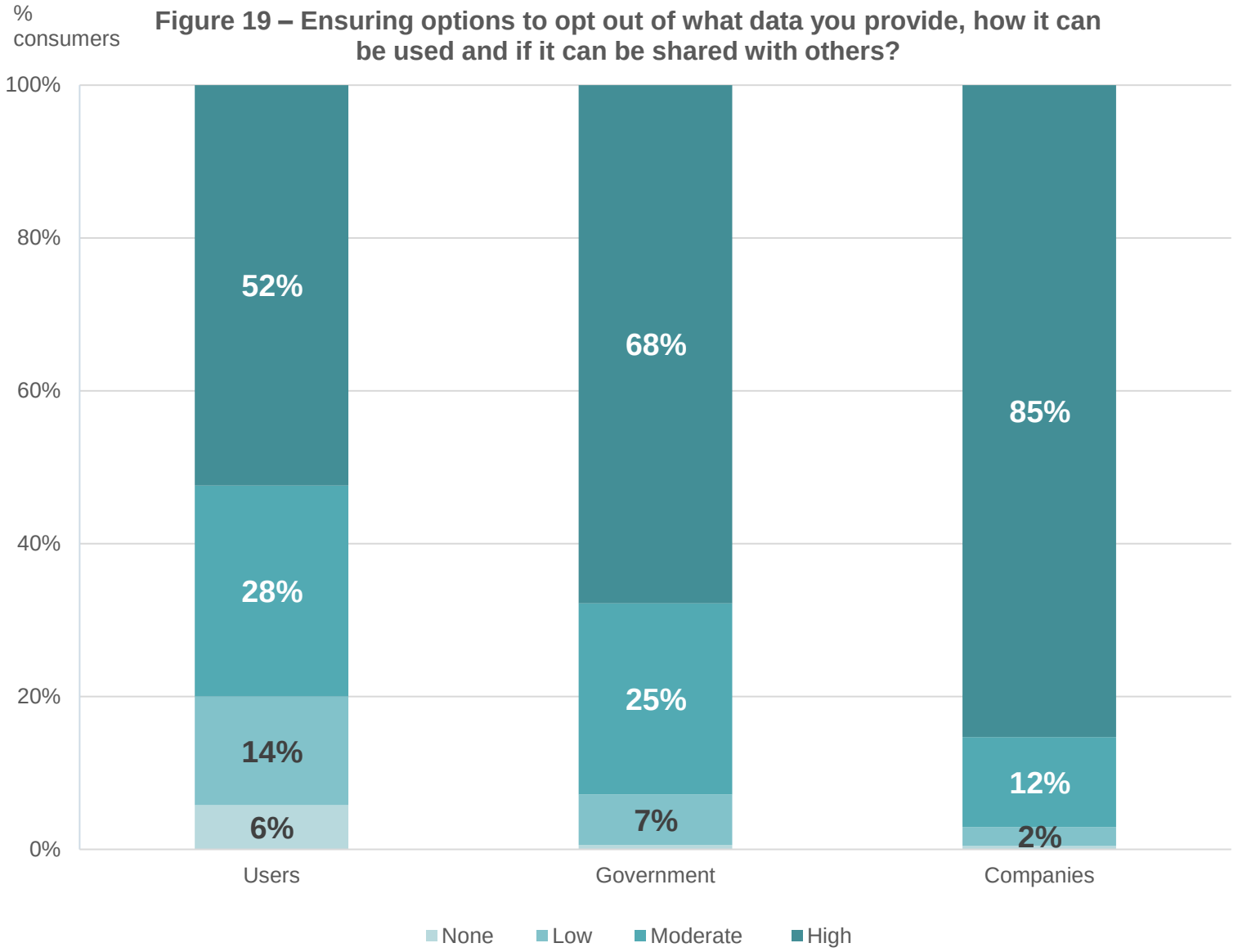
85% of consumer feel companies have the highest level of responsibility in ensuring they have options to "opt out" of different data collection, use and sharing practices

These results aligned with consumer sentiment regarding whether companies should give options to opt out of certain types of information they can collect, use and share (95% agreed with this – see Figure 10, p. 22).

"It's just they literally make you jump through hoop after hoop to get it done. Just make it simple to opt out. Make it clear, make it obvious, make it easy."

85% consumers think companies have a high level of responsibility to ensure there are options to opt-out

Figure 19 – Ensuring options to opt out of what data you provide, how it can be used and if it can be shared with others?



Q: What level of responsibility do you think each of the following (Users/Government/Companies) should have in relation to:

***Note** – data labels ≤ 1% are not shown*

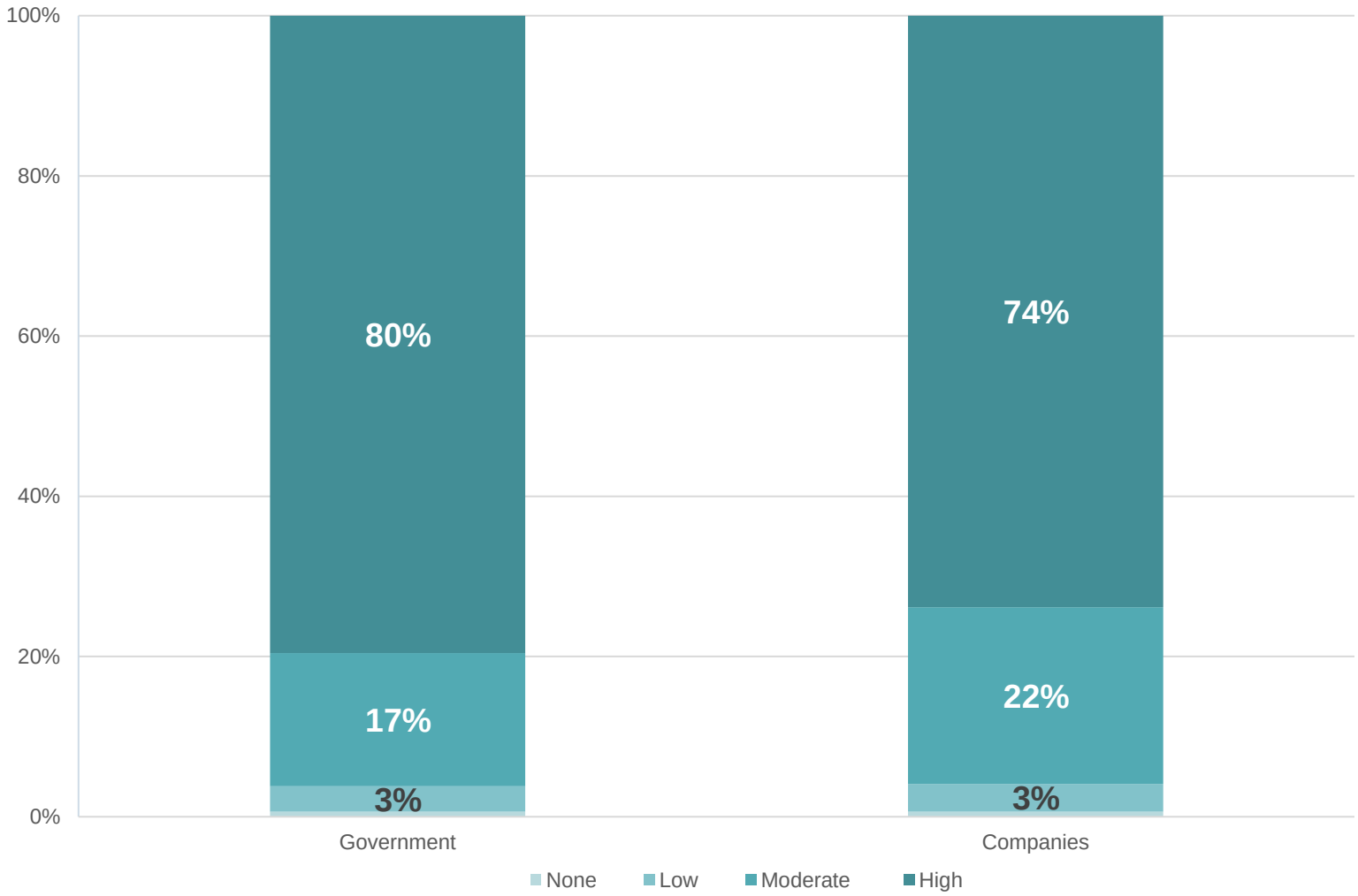
Consumers are looking to government to develop protections to prevent profiling that leads to exclusionary outcomes – with 80% feeling government has a high level responsibility in this space

Consumers by no means feel companies have no role in preventing exclusion, with 74% feeling they also have a high level of responsibility in relation to this issue.

"I suspect there are (rules in place), but I don't really know… The industry may have done some sort of Code of Behaviour, I guess. But when industries can't even pay people the proper award rate; well, I don't have much faith in them self-regulating with this sort of stuff…

80% consumers think government has a high level of responsibility to develop protections that prevent exclusionary outcomes

Figure 20 – Developing protections to ensure no one is excluded from essential products or services (e.g. electricity, gas, telecommunications) based on their data and / or profile?



Q: What level of responsibility do you think each of the following (Government/Companies) should have in relation to:

***Note** – data labels ≤ 1% are not shown*

Part Four

Consumer policy insights

COVID-19 has accelerated growth of consumer participation in online environments and digital marketplaces

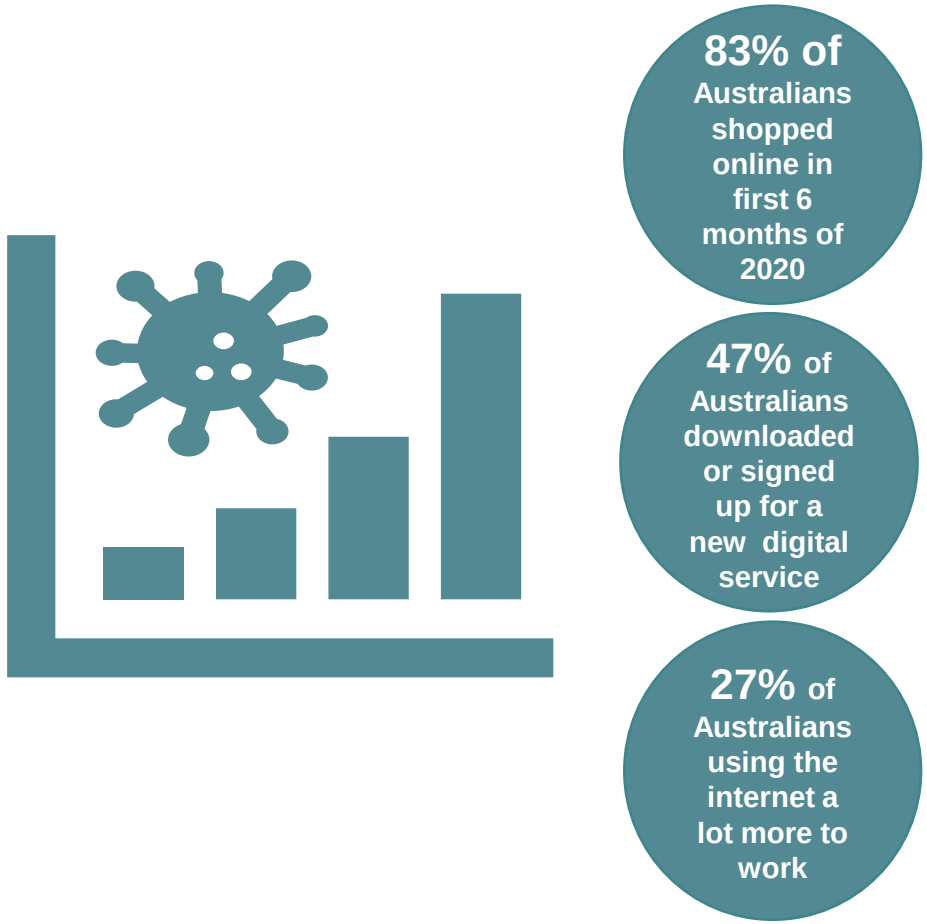
The COVID-19 pandemic, and associated public health restrictions, has meant that many consumers are spending more time online for work, education, shopping, socialising and entertainment (see p. 15).

Digital marketplaces and innovations are providing clear benefits to consumers and the economy during COVID-19. However, the risks consumers face online and in digital marketplaces are heightened by increased usage of digital products and services, and subsequent increased volume of their personal data being collected by companies.

As outlined in CPRC's ***Consumers and COVID-19: from crisis to recovery*** research report – the pandemic has also created circumstances in which consumers are more exposed to exploitative practices online (in particular – scams, false claims, unsafe products and price gouging).

COVID-19 has increased the urgent need for reforms to Australia's consumer protections framework, so consumers aren't relying on analogue safeguards in an increasingly digital world.

Figure 21 – Changes in consumer behaviour due to COVID-19



At a time when reliance on them is growing, digital marketplaces have some serious shortcomings

Consumer engagement with Privacy Policies and T&Cs (that dictate how consumers' data is collected, shared and used when participating in digital marketplaces) has not improved in the past two years (see p. 18). At the same time, consumer discomfort and opposition regarding the data practices that Privacy Policies and T&Cs can permit has grown (see Figure 22).

These survey results back up the findings of the ***Australian Competition and Consumer Commission's Digital Platforms Inquiry*** (pp. 449 - 455) . This inquiry found that company data practices are often characterised by:

- **Information asymmetries** that undermine a consumer's ability to assess whether services align with their privacy preferences
- **Bargaining power imbalances** that prevent consumers making genuine choices on how their personal information is collected, used and shared
- **Behavioural biases** that work against consumers' ability to select privacy options that better align with their privacy concerns

Australia's consumer protections need to be modernised so that consumers are protected against practices that unfairly exploit information asymmetries, bargaining power imbalances and behavioural biases.

Figure 22 – Changes in consumer attitudes regarding data handling practices

% of consumers who…	2018	2020
Agree it is enough to notify them how data is collected and used via Privacy Policies and T&Cs	37%	33%
Consider it very unacceptable to monitor online behaviour to show relevant ads	29%	35%
Consider it very unacceptable to charge people different prices based on past purchase / online browsing / payment behaviours	77%	81%
Consider it is very unacceptable to collect data without their knowledge to assess their eligibility or exclude them from loans or insurance	76%	79%

There's a chasm between how consumers expect to be treated in – and the practices that characterise – digital marketplaces

There is a disconnect between consumer expectations about being treated fairly, and many of the data handling practices that are common in digital marketplaces (see p. 25 and Figure 23).

Maintaining the regulatory status quo will not only cause this disconnect to widen, but it will also increase risks of direct consumer harms – whereby consumers are treated unfairly and/or have their privacy and safety compromised. These outcomes will erode trust and confidence in digital technologies and marketplaces.

Consumers feel that both companies and government have high levels of responsibility for ensuring they are protected in digital marketplaces. Reforms need to set clear standards of fairness, inclusion, safety and privacy– and incentivise companies to compete on this basis.

Reforms to consumer protections – such as unfair trading practice and contract term prohibitions, and a general safety provision, being added to Australian Consumer Law – as well updates to the Privacy Act, need to be progressed without delay.

Figure 23 - Common company data practices consumers considered to be unfair

Having their personal information being used to make predictions about them	**76%**
Companies collecting information about them from other companies	**83%**
Companies sharing personal information consumers have provided with other companies	**85%**
Companies selling personal information consumers have provided to other companies	**90%**
Requiring more personal information than necessary to deliver products/services	**88%**

For more information about this research please do get in touch.

office@cprc.org.au

Level 14, 10-16 Queen Street

MELBOURNE, VICTORIA 3000

T 03 9639 7600 W cprc.org.au

Consumer Policy Research Centre