

Deloitte.



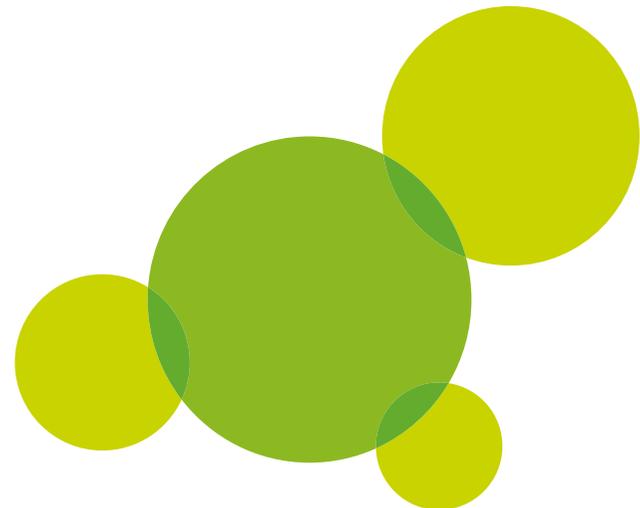
**Seeing beyond the
surface: The future of
privacy in Australia**

Deloitte Australian
Privacy Index 2021



Contents

1. Foreword	04
2. About the report	05
3. Key findings	07
4. Top five takeaways for brands	08
5. Privacy Index 2021	09
6. The right to request erasure	11
7. AI and automated processing	13
8. Targeted online advertising	16
9. Methodology	20
10. References	21



“Strong data protection and privacy rights are both necessary to uphold our human right to dignity in the digital age, and a precondition for consumer confidence and economic growth.”

OAIC submission in response to the Attorney General’s Issues Paper, December 2020



1. Foreword

The world is a very different place today compared to a year ago. The pandemic has had a dramatic impact all over the world, to all aspects of life and wellbeing. As we were confined to our homes, technology has had to move even more rapidly than usual to ensure that we could stay functional, connected and productive. And we too have had to adapt, adopt and accept in order to live in this new world. Online shopping, contactless payments, remote working and virtual or digital health care are a few of the technology trends that have become ingrained habits.

Consumers needed organisations to meet them in the virtual confines of their homes, and to a large extent, they did. But this digital acceleration came with an impact on the privacy of individuals. Even more than before, our digital habits, health, interests, and curiosities have not only been tracked, but shaped what is presented back to us. To be fair, this is often positive and not just a potential cause for concern, so we wanted to hear from Australian consumers on the topic.

The pandemic did not merely cast a light on data privacy, it accelerated the focus on this essential human right. In a world that moved into all things digital at lightning speed, data privacy has become a non-negotiable – as it should be.

The last 12 months have heightened the importance of privacy in many ways. The increase in high-profile data breaches has raised consumer awareness about the importance of their privacy and has provided them

with greater understanding of what it means to them. Consumers have been able to better identify the brands they do and don't trust to handle their personal information online, which hasn't been confined just to the realm of distrust in social media. Consumers have been expressing frustration across industries in their desire to take back control of their personal information.

This digital acceleration puts pressure on global privacy laws to adequately protect the rights and freedoms of consumers. Australia is in the privileged position of having our legal review and reform process still in progress, meaning this digital acceleration can be factored into the future protections we afford to Australian consumers.

The initial direction of this legal review and reform was indicated in the Attorney General's Issues Paper that was released last year. The themes in this Paper resemble those embodied in the *European Union's General Data Protection Regulation*, but given the acceleration of the digital economy, do these protections go far enough?

In this year's Index, we look at some of the technologies that are supporting our digital acceleration, and the capabilities that impact consumers' control over their personal information, to understand how consumers want to be protected by their future privacy regulation. Specifically, we have focused on the future of privacy relating to the increased use of Artificial Intelligence (AI) across industry, the future of targeted online advertising through cookies, and the potential of the right to erasure to offer consumers greater control over their personal information.

In this report, consumers have provided a clear view of how they would like to control their personal information that is used by AI and collected through cookies. However, under the current legal framework, this level of control is not supported by industry. Our research also shows that consumers would feel more in control of their personal information if the right to erasure were to be introduced.

We have made the insights highlighted in this report available to the Attorney General to support their review of the *Privacy Act 1988* (cth). We hope these insights will support this review, to enable the future Australian privacy legislation to better address consumer concerns, and meet consumer expectations, across our increasingly digitised economy.



Daniella Kafouris
Partner
Deloitte



2. About the report

2.1 Introduction

In July 2019, the ACCC published the Digital Platforms Inquiry, finding that the current regulatory frameworks governing the processing of data in Australia do not adequately consider the digitisation of the economy and the monetisation of consumer data through targeted advertising. The ACCC stated that the *Privacy Act 1988* (Cth) (henceforth referred to as the Privacy Act) needs reform to inform, empower and protect consumers about how their data is being collected and used.

This inquiry sparked the announcement by the Attorney-General that the Australian Government would conduct a review of the Privacy Act to ensure that privacy regulation effectively empowers consumers, protects their data and best serves the Australian economy. This review was delayed by the COVID-19 pandemic but is now back in government focus.

In October 2020, the Attorney-General released an issues paper consisting of 68 questions and invited submissions to these, for consideration in the government's review of the Privacy Act. The questions covered a range of topics across privacy including, but not limited to:

- the scope and application of the Privacy Act;
- whether the Privacy Act effectively protects personal information; and
- whether individuals should have a direct right of action to enforce privacy obligations.

The questions outlined in this issues paper have formed our thinking for this year's Index and will likely shape the future of privacy in Australia.

For the purpose of this Index, we have limited our considerations on the future of privacy to:

- the possible impacts of introducing the **right to erasure**;
- the increased use of **artificial intelligence (AI)** and what this means for the future privacy regulatory landscape; and
- the use of and perceptions about **targeted online advertising** and how consumers want to be protected in this space.

We sought to gauge what consumers would value in an updated Privacy Act and how they would respond to additional rights that might be afforded to them, to help inform the regulatory review and provide insights to brands into their consumers' values.

2.1.1 The right to erasure

For the purpose of the consumer survey we defined the right to erasure as: "an individual's ability to request a brand to delete all personal information it holds about them and requires the brand to do so, unless exceptions apply".

We asked consumers:

- whether they were aware of what a right to be forgotten allowed them to do;
- whether they would use this right if it were afforded to them; and
- which industries they would most likely use the right to be forgotten on.

We also asked our clients how many individual rights requests they currently receive and whether they are concerned about having to implement the right to be forgotten in the future.



2.1.2 Artificial intelligence (AI)

We defined AI for the participants of the consumer survey as: “Artificial intelligence, also known as AI, is the programming of a machine or computer so that it thinks like a human and can automatically solve problems or perform tasks without human guidance.”

We asked consumers:

- whether they are concerned about the use of AI across society;
- what they are most concerned about; and
- how brands can alleviate these concerns to build trust.

We analysed the websites of 50 leading Australian consumer brands to understand which brands are informing consumers about the use of AI and we surveyed our clients to understand what proportion of leading consumer facing brands are using AI.

2.1.3 Targeted online advertising

We defined targeted online advertising as: “When an organisation matches the adverts shown to an individual to that individual’s habits and interests as collated from their online activities”. Organisations can do this by using internet cookies that track an individual’s browsing history to build up a picture of that individual’s interests and values.

We asked consumers:

- whether they would like the information that is used to track them online to be protected under the Privacy Act;
- how concerned they are about internet cookies that track them online for marketing purposes and are sold on to third parties; and
- how they want to be able to manage their online preferences.

We analysed websites of 50 leading Australian consumer brands to understand how easy, or otherwise, it was to limit the use of tracking and marketing cookies. We also asked our clients whether their privacy teams are involved in cookies and other marketing decisions.

2.2 The Index

This year we analysed brands by assessing their website and privacy policies for cookie use and transparency in notifying consumers about the use of AI. We also surveyed some of our leading consumer serving clients to understand their current privacy practices and concerns over any future introduction of the right to be forgotten. We combined the findings of this brand analysis with selected findings from the consumer survey, as well as sector level breach and complaints data published by the Office of the Australian Information Commissioner (OAIC). The results were scored and aggregated across 10 industry types enabling us to rank each industry to create the Index.

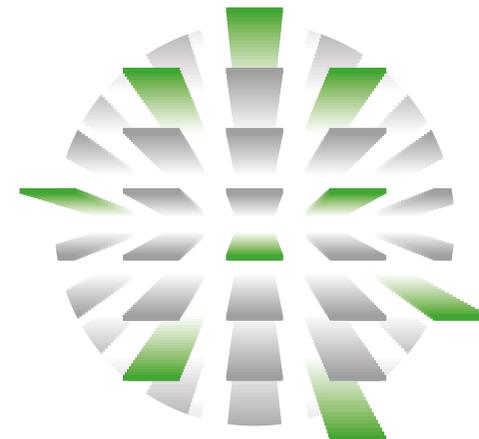
2.3 Results

All survey responses are confidential and anonymised. The Index and accompanying report aggregate responses statistically analysed to provide insights into key consent practices across the 10 identified industry groups compared to the consent expectations of consumers.

2.4 Acknowledgements

We would like to acknowledge the following for their support:

- Roy Morgan Research Ltd for conducting the consumer survey on behalf of Deloitte.
- The participants of the consumer survey for providing their responses.
- Our clients who participated in the Brand survey for providing critical insights into their industries.



3. Key findings

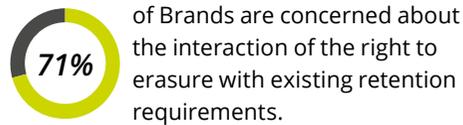
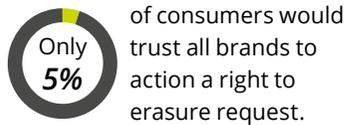
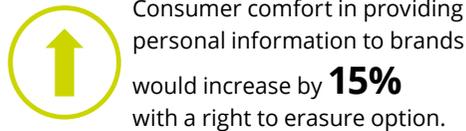
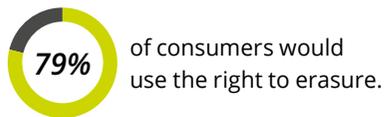


Consumers are concerned about how their privacy is handled online and want brands to be more transparent.

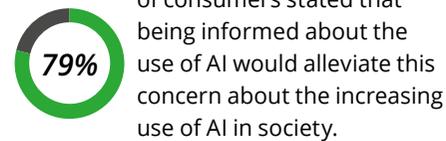
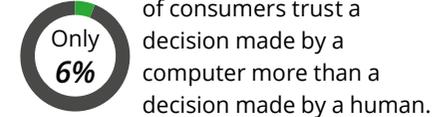
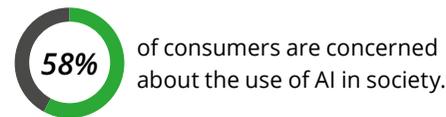
3



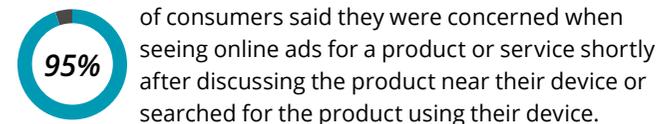
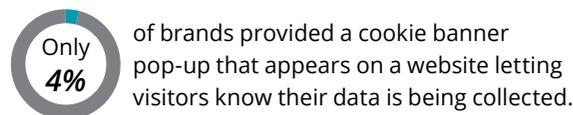
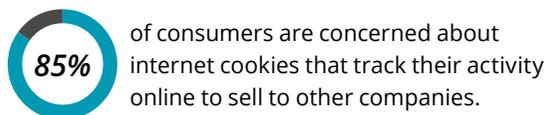
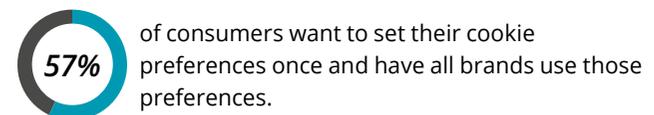
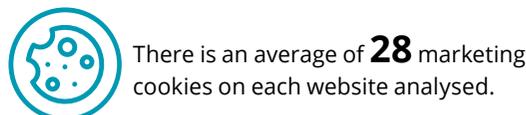
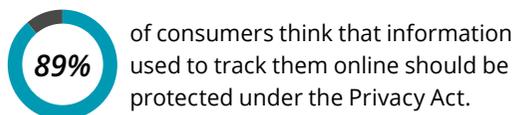
Right to erasure



AI and Automated Processing



Targeted online advertising



1

2

4

5

6

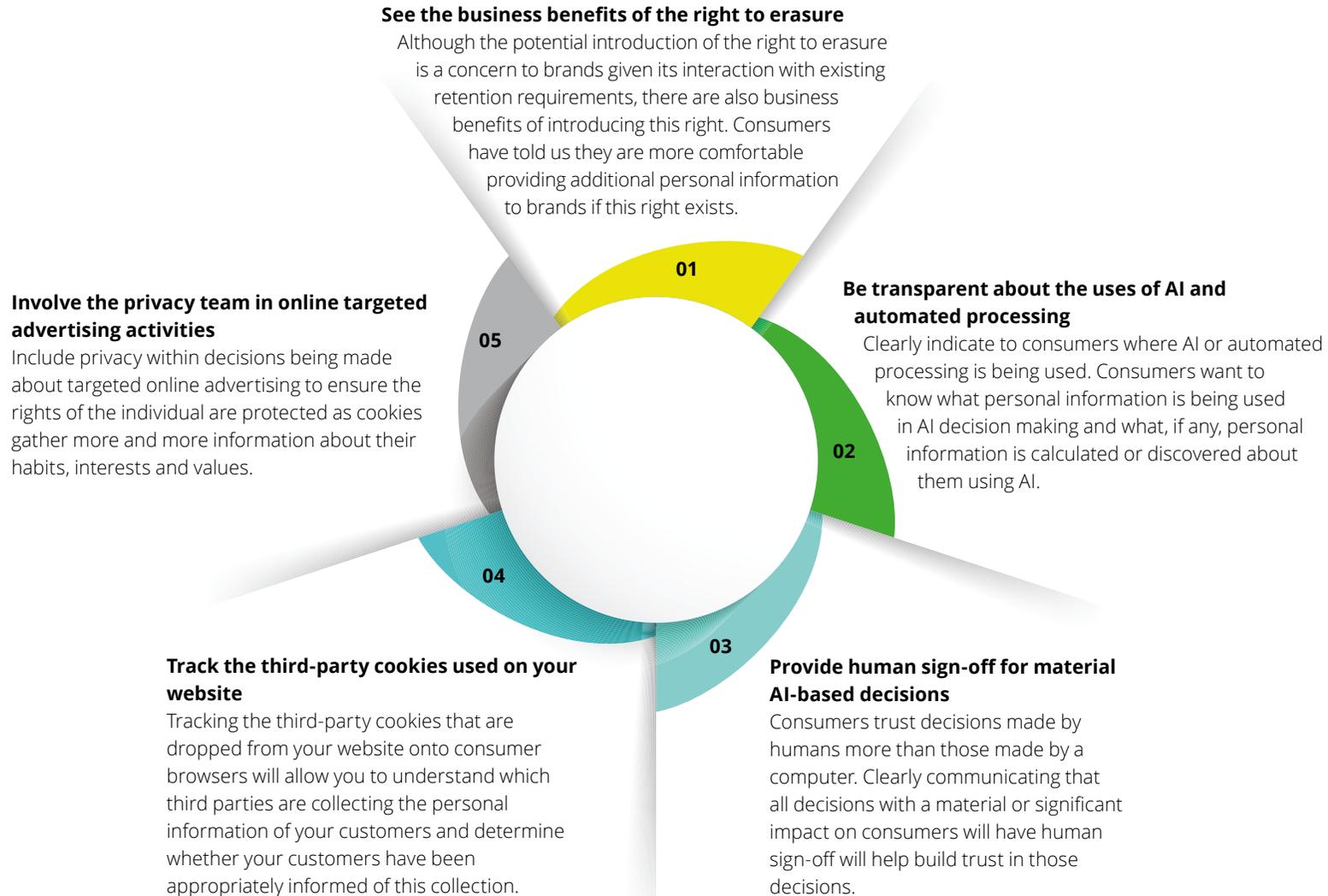
7

8

9

10

4. Top five takeaways for brands



- 1
- 2
- 3
- 4**
- 5
- 6
- 7
- 8
- 9
- 10



5. Privacy Index 2021

How each sector ranked

5.1 Overall Index

Index Focus	Current Ranking		Previous Rankings	
	Future of Privacy	Consent	Apps	Notice
Sector	2021	2020	2019	2018
 Information Technology	1	3	1	9
 Government	2	2	8	2
 Travel and Transport	3	4	3	N/A
 Education & Employment	4	6	6	11
 Retail	5	1	5	7
 Real Estate	6	5	2	8
 Health & Fitness	7	10	10	6
 Financial Services	8	9	9	1
 Energy & Utilities	9	7	4	4
 Telecommunication & Media	10	8	7	3

Each year the Index focuses on a different privacy element and as such should not be treated as a like for like comparison. Rather it should be seen as a holistic view of each industry's privacy posture across each year's Index focus area. For example, the Retail sector had leading practices around consent (the focus of 2020's Index) as compared to other industries, but ranked in the middle with regards to application privacy (2019's focus) and the future of privacy (this year's focus).

By focusing on the future of privacy in the 2021 Privacy Index, the sector rankings have once again shifted. The Information Technology industry has jumped from 3rd to 1st position, while Retail has fallen from 1st to 5th position. Positions 8, 9 and 10 are taken up by Financial Services, Energy & Utilities and Telecommunications & Media respectively. These rankings are perhaps unsurprising when focusing on the future of privacy in Australia. Those industries that have dominated market share historically (e.g. Financial Services and Energy) have legacy systems that may experience difficulty with upcoming changes to the Privacy Act, whereas the industry that is largely driving technological advancement across Australia (Information Technology) may be better placed to pivot to new individual rights or requirements around AI and online advertising.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10

5.2 Trust in privacy

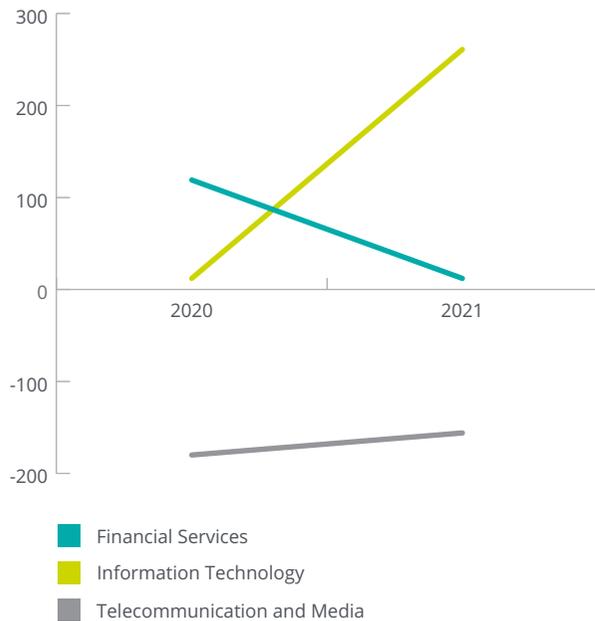


Fig. 1 Changes in Privacy Trust in the last year

Each year we ask 1,000 consumers which brands they trust the most and which they trust the least with their privacy. Those results are then aggregated across industry sectors, returning a net negative or positive trust in privacy score. This score per industry for 2021 has been compared against the 2020 results, where the highest scoring and lowest scoring industries (Financial Services, Information

Technology and Telecommunication & Media) can be seen in Figure 1. The remaining industries all had a similar number of trusting and distrusting consumers over the last year, so their lines on this graph would converge on zero if shown.

The major movers in this year's trust in privacy measurement have been the Financial and Information Technology industries. In 2020 Financial Services brands were the most trusted by consumers, however the number of consumers that named Financial Services brands in 2021 was minimal. By comparison trust in Information Technology brands has increased significantly over the last year. This is possibly due to Information Technology brands using privacy as a selling point to their customers.

The Telecommunications and Media sector as a whole remains in its position as the least trusted by consumers overall, albeit on a positive trajectory, and in large part because this sector includes social media brands. For 2021, **78%** of consumers that distrust this industry named social media brands as those they trusted least compared with **94%** in 2020. This is not surprising as trust in social media brands is still recovering from several high-profile data breaches and negative press in recent years.

Away from the specific brands and industries, we also provided the 1,000 consumers the opportunity to nominate trust in all brands or no brands. Figure 2 shows that the percentage of consumers that trust no brands has decreased, while the percentage that trust all brands has increased slightly, between 2020 and 2021. Also, the percentage of consumers that couldn't think of any

brand to trust has reduced over the last year, while the percentage of consumers that could name a specific brand to trust has increased roughly **60%** on the 2020 results. These findings suggest that consumers are becoming more aware of the brands that they do trust, indicating an increased awareness of and value placed on privacy.

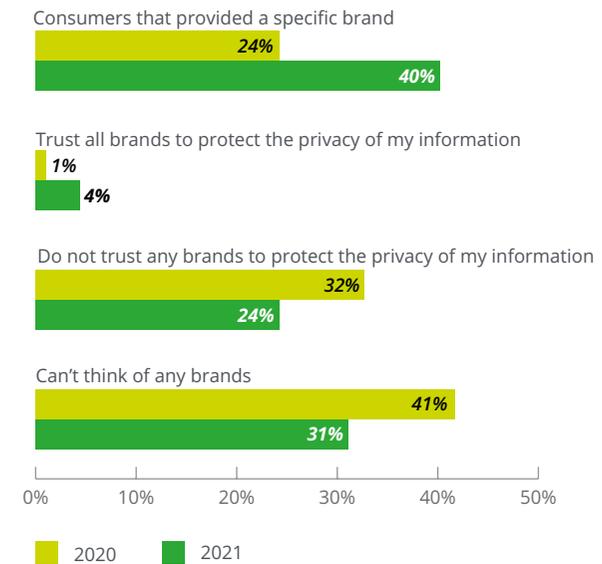


Fig. 2 Overall trust between 2020 and 2021



6. The right to request erasure

Consumers are overwhelmingly in favour of having greater individual rights when it comes to their personal information. A right to erasure can support more effective information sharing and presents an opportunity for brands to foster greater trust with their consumers.

6.1 A global privacy trend

A 'right to erasure', also commonly referred to as a 'right to be forgotten', is already an established individual right under the European Union *General Data Protection Regulation* (henceforth referred to as the GDPR) and several other regional privacy regulations.

The ACCC has suggested that enabling consumers to request erasure of their personal information will provide them with greater control over this information and is likely to help mitigate the bargaining power imbalance between consumers and the brands that they interact with.¹

We asked questions of consumers to understand how they would be likely to engage with a right to erasure, including whether the right would foster greater trust between consumers and brands.

6.2 The value of a right to erasure

Consumers overwhelmingly support the establishment of a right to erasure within the Privacy Act, with **79%** of consumers surveyed indicating they would either be 'likely' or 'very likely' to use a right to erasure.

How likely would you be to use the right to erasure if it was included in Privacy Act?

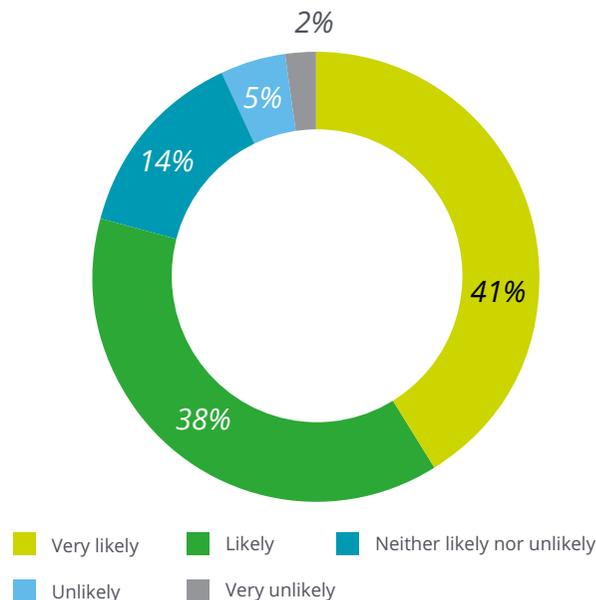


Fig. 3 How likely consumers are to use a right to erasure

Consumers also highlighted that there are a number of different reasons why they would be likely to use a right to erasure. The most popular reasons that would motivate surveyed consumers to use such a right include receiving

too many marketing emails and updates (**84%**), not wanting a brand to hold onto their personal information after they stop dealing with the brand (**80%**), and not trusting the brand to use personal information responsibly (**73%**).

When asked for the main reason to use this right, the leading response from consumers was a lack of trust in a brand. This indicates that the most important thing to consumers is that brands use and store their information responsibly, and it highlights that consumers see a right to erasure as a way of having more control over their personal information.

6.3 Addressing the imbalance of power and building trust

Our consumer research suggests that the right to erasure has the potential to address power imbalances between consumers and brands and have a positive impact on trust between them. We have found that an established right to erasure has the potential to increase the willingness of consumers to share their personal information with brands.

Although **26%** of consumers indicated that they currently felt comfortable providing their personal information to the brands that they deal with online, **41%** indicated that they would feel comfortable providing additional personal information to those same brands if a right to erasure was in place that would allow them to request that their personal information be deleted at a later stage.

1. ACCC, Digital Platforms Inquiry Final Report, July 2019, p471.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10



Which, if any, of the following industries are you likely to make a right to erasure request to?

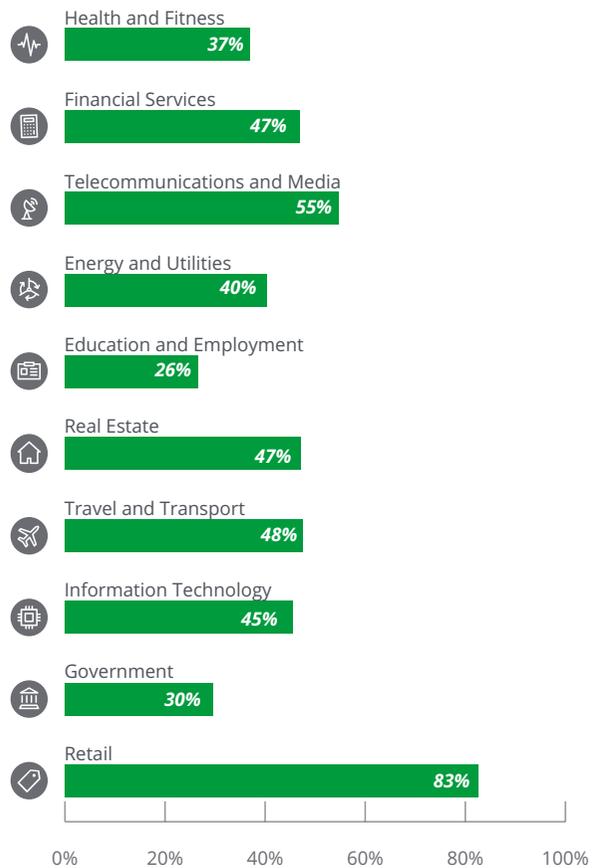


Fig. 4 Industries consumers would like to make erasure requests to

This **15%** increase in consumers willing to share additional personal information highlights the potential of a right to erasure to foster trust and lead to better outcomes for both consumers and brands.

Consumers appear to see the greatest value in exercising a right to erasure when interacting with brands in specific industries.

Our results indicate that industries which frequently collect, use and disclose personal information for non-essential activities are particularly likely to attract requests for erasure from consumers.

83% of consumers indicated that they would use a right to erasure with brands in the retail industry, many of which collect significant amounts of personal information in the delivery of e-commerce, customer loyalty programs, marketing, and promotions.

In contrast, consumers are less likely to exercise a right to erasure when dealing with the industries that they typically engage with over sustained periods, as well as those that they trust the most. Consumers indicated that they would be less likely to exercise a right to erasure when dealing with organisations and brands in the Education and Employment (**27%**), Government (**30%**) and Health and Fitness industries (**37%**).

Despite the potential for this right to address the bargaining power imbalance between consumers and brands, consumers remain sceptical about the willingness and capabilities of brands to action such requests.

When asked whether they would trust brands to action a right to erasure request, **20%** of consumers indicated that they would not trust that any brands would delete their personal information on request. Just **5%** of consumers indicated that they would trust all brands to delete their personal information in accordance with a right to erasure request. This highlights that even though the existence of a right to erasure within the Privacy Act may lead to greater control for consumers and more sharing of personal information, in order to foster trust between consumers and brands, it will be just as important to ensure brands are able to follow through and implement processes and capabilities to respond to an erasure request.

Indeed, there are likely to be some key implementation considerations for brands should a right to erasure be introduced. Of our surveyed clients, **57%** indicated that only a 'few' or 'some' of their systems currently have erasure capabilities and processes, and **71%** indicated they were either 'concerned' or 'very concerned' about how this right would interact with legislative data retention requirements.

6.4 Greater awareness will be key

Of consumers surveyed, only **17%** indicated that they were familiar with a right to erasure before completing the survey. This is understandable given that there is currently no direct equivalent to such a right under the current Privacy Act. However, if the benefits the ACCC identifies in a right to erasure are to be realised, greater awareness of this right is needed. It will be important for brands to engage with consumers and ensure they understand what it is, and how it can be used.

- 1
- 2
- 3
- 4
- 5
- 6**
- 7
- 8
- 9
- 10

7. AI and automated processing

Artificial intelligence (AI) has grown significantly in recent years as brands seek to leverage the power of its evolving capabilities.² Consumers have concerns over the use of AI, and brands can alleviate their concerns and build consumer trust through being transparent and by ensuring data accuracy.

7.1 Consumer awareness around AI

Our survey found that **89%** of consumers have some awareness of AI. This awareness is high across all age groups; however, some age brackets are more aware of AI than others. For example, **92%** of those aged 18-24 years are aware of AI as opposed to **86%** of those aged 65+.

Have you heard of Artificial Intelligence ?

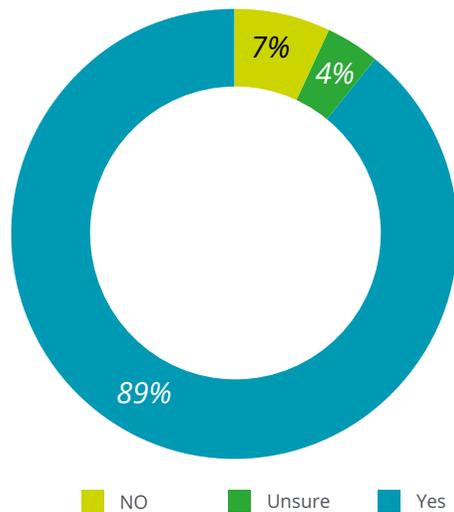


Fig. 5 Consumer awareness about Artificial Intelligence

We then asked these consumers what they know about AI. **53%** understand that AI can be used to track and use information about them. However, **32%** of consumers are still unsure about what AI was even though they had “heard of it.” This suggests that greater awareness is needed about the commercial uses of AI before consumers are able to make informed decisions about AI that uses their personal information. However, our brand research found that **71%** of privacy policies do not mention AI.

Consumers were also asked to consider which industries indicated AI was being used to assist them with purchasing a product or service. Consumers are aware of AI being used in Information Technology (**43%**), Telecommunications and Media (**26%**), Retail (**26%**) and Travel and Transport (**22%**). This is intuitive as consumers will likely engage with many brands within these industries and the use of AI within these industries is more commonly known.

Consumers were not as aware of AI being used in Financial Services (**19%**), Real Estate (**16%**), Energy and Utilities (**13%**) or Education and Employment (**12%**). This is concerning as often interactions with these industries can have significant impacts on the livelihood of consumers. For example, a bank could deny a loan application or an employment hire could be rejected based solely on automated decision making.

2. Deloitte, Conversational AI: Conversational AI is powering the next wave of customer and employee experiences 2019, p13

Which industries informed you about the use of Artificial Intelligence (AI) when buying a product or service?

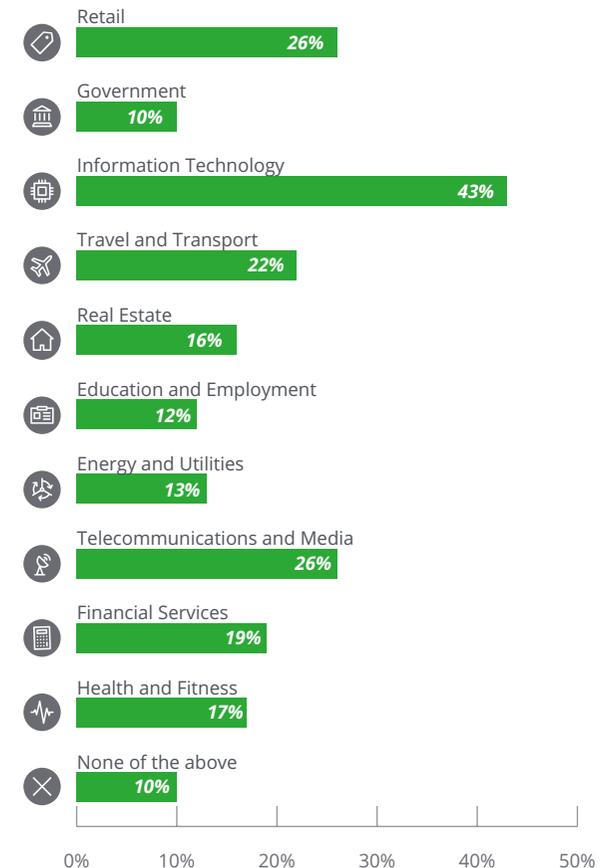


Fig. 6 Consumer perception of being informed about AI

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10

A factor to consider in understanding this data is that it is based on consumer perceptions of when AI is being used. Consumers are likely to have interacted with more brands from the industries that rated highly than with those that didn't (e.g. consumers interact with many Retail brands, but likely to interact with just one or two Energy or Utility brands).

7.2 Trust – Humans vs Machines

Our research found that although consumers have demonstrated a reasonably broad awareness of AI, this has not translated into consumer trust in AI based decisions or a brand's use of AI. Nearly half of consumers trust a decision made by a human more than a decision made by a computer. Only **6%** of consumers were willing to trust a machine more than a human. This paints a stark picture for consumer trust in a brand's AI based decisions as none of the brands researched stated within their privacy policy that all AI decisions had human sign-off. There is a risk that consumer trust in brand decisions could decrease as brands increase their automated, computer-based decision-making.

Consumers were asked to indicate all industries they trust to use AI responsibly as well as which single industry they trust the most. The responses to these questions identified Government as the most broadly and strongly trusted industry when it comes to the use of AI. Specifically, **28%** of consumers included Government within the list of industries that they trust to use AI responsibly, compared to **18%** for Retail and **15%** for Information Technology.

Are You More or Less Likely to Trust A Decision Made By a Human, or an Artificial Intelligence (AI) Decision Made By a Computer?

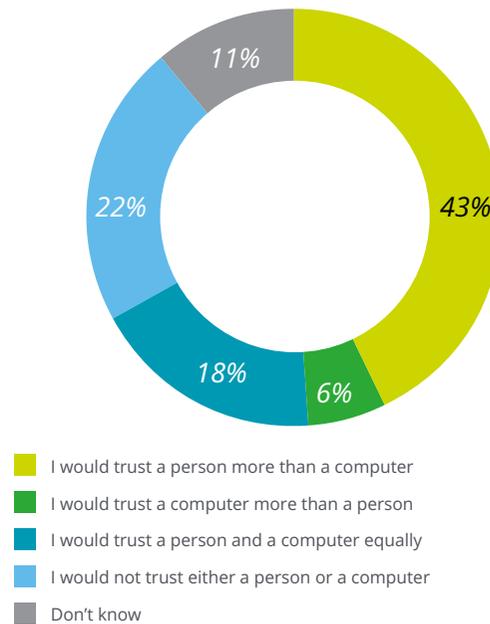


Fig. 7 Consumer trust in human and computer based decisions

Interestingly, **52%** of consumers did not trust any of these industries to use AI responsibly. This is concerning as this statistic suggests industries are not doing enough to ease concerns about AI. However, of those that did trust an industry, **40%** trust Government the most.

% of consumers concerned about Artificial Intelligence (AI) by age

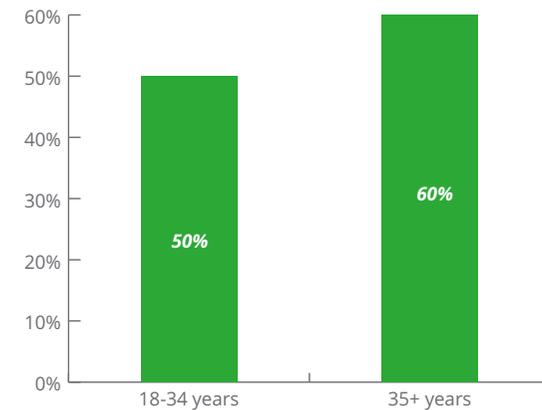


Fig. 8 Percentage of consumers concerned about the use of AI in society

7.3 Concerns around AI

58% of consumers are concerned about the growing use of AI across society. Unsurprisingly, younger consumers are less averse to the use of AI across society with roughly **10%** fewer 18-34-year-olds reporting concern compared to those over 35.

When looking to understand this concern about the use of AI across society we identified two central themes: transparency and accuracy. **77%** of consumers indicated concern about not being informed when AI is being used to process their personal information, aligning to the theme of transparency.



These transparency concerns are justified as **69%** of consumers stated they had never been told about the use of AI when buying a product or service online. This causally links to our brand analysis, as only **14%** of researched privacy policies called out the specific decisions made by AI. Brands will need to do more in this space to create greater levels of transparency.

Accuracy has been identified as a theme of concern because **80%** of consumers are concerned about decisions being made by AI using inaccurate information and **79%** of consumers are concerned by the inability to challenge an inaccurate decision made by AI. Our brand research validates these concerns as only **3%** of brands called out how to challenge AI decisions specifically in their privacy policy.

Our analysis also showed that only **69%** of consumers are concerned with AI replacing jobs in the workforce, which is one of the lower rated concerns captured in the research. This is an interesting finding as it conflicts with common thinking of consumer perceptions in this space.

7.4 How to Build Trust

Alleviating consumer concerns about the use of AI would build consumer trust in AI-based decisions and in the brands that use them.

77% of consumers who are concerned about AI stated that brands being transparent about the use of AI would lessen these concerns. The OAIC has recommended that data transparency be improved through introducing

standardised industry wide icons and a lexicon to assist consumers to make informed decisions about their personal information.³ A standardised symbol for automated processing and the use of AI could increase transparency and consumer awareness.

Being transparent is particularly important to those brands whose target audience are consumers over the age of 50, as a higher proportion of consumers in that age group said that transparency would lessen their concerns about AI.

Consumers have outlined what information they would like brands to be transparent about. The most popular of which include:

- Providing the personal information involved in the AI decision making process (**68%** of respondents).
- Providing consumers with any personal information about them that is calculated by or predicted by the AI technology (**62%** of respondents).
- Notifying consumers of any personal information discovered by the AI (**58%** of respondents).

To address accuracy concerns, most consumers want clear guidance on how to challenge AI decision making (**67%**) and to limit AI to basic tasks that do not have a major impact on people (**59%**). If brands implement these changes, they will build consumer trust while also reaping the commercial advantages of implementing AI.

3. OAIC – Privacy Act – Submission to the Issues Paper. December 2020, Pg 74

What sorts of things concern you about the use of Artificial Intelligence (AI) in our society?

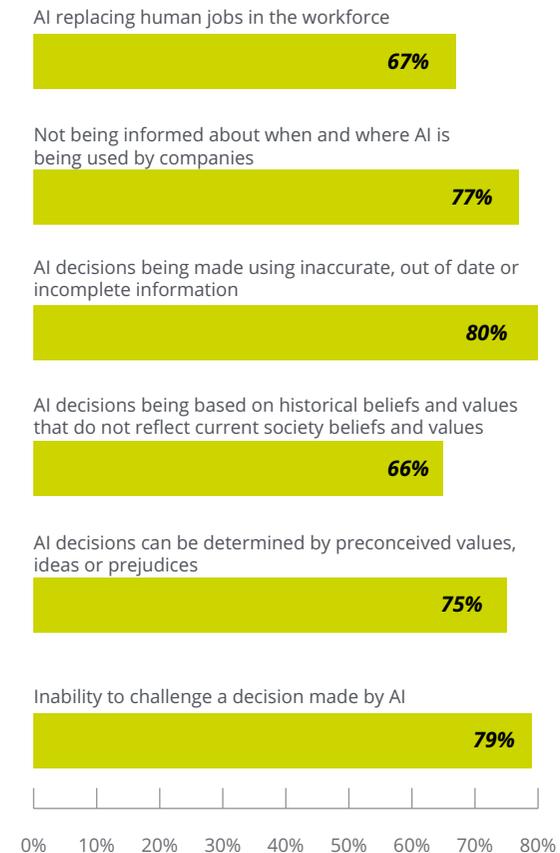


Fig. 9 Types of consumer concern about AI

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10

8. Targeted online advertising

The use of tracking cookies has greatly expanded the modern marketer’s tool kit, allowing them to target customers with tailored ads, but this online ‘surveillance’ has led to consumer concern. The question for companies is how they can implement targeted advertising without triggering concerns about privacy or provoking consumer opposition.

8.1 Protection under the Privacy Act

The Privacy Act applies to personal information, which is defined in the Act as “information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.” The data collected by marketing cookies allows advertisers to build up a picture of an individual’s habits and interests based on the websites they visit; however, these interests and habits are often not enough to identify the individual. As a result, in Australia, information collected by cookies may not be protected by the Privacy Act.

In contrast, consumers are overwhelmingly in favour of having their information that is collected by cookies and other tracking technologies protected by the law. Indeed **89%** of customers agree that information used to track them online should be protected under the Privacy Act.

Do you agree or disagree that the information used to track you online should be protected under the Privacy Act?

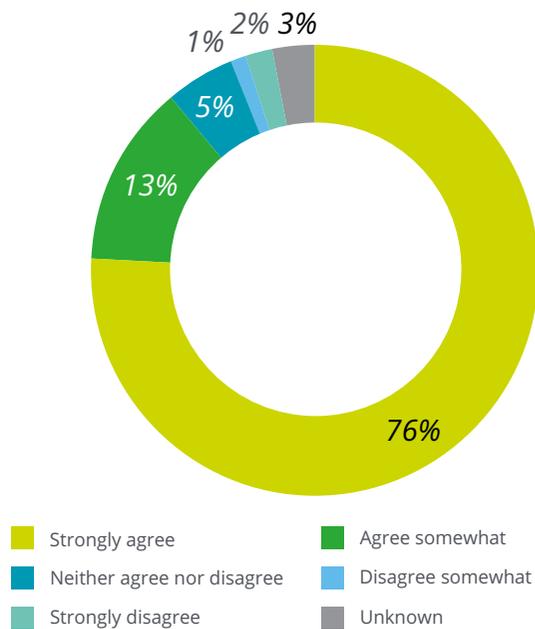


Fig. 10 Consumer sentiment towards protecting cookie information

8.2 Consumer concern about cookies

This desire to have cookie data protected under the Privacy Act seems to be particularly driven by consumers’ concern over cookies tracking their online activity, with **74%** of consumers highlighting their concern about brands that use internet cookies to track their activity online to market to them, whilst **85%** are concerned that brands sell information gathered by internet cookies to other companies. This sentiment indicates that consumers, if provided the choice, would not currently consent to marketing and tracking cookies being used to collect information about them, signalling that organisations need to be more transparent in order to build consumer trust so that customers feel comfortable consenting to these cookie practices.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8**
- 9
- 10

"I am concerned about cookies that track my activity online and use this information to market to me"

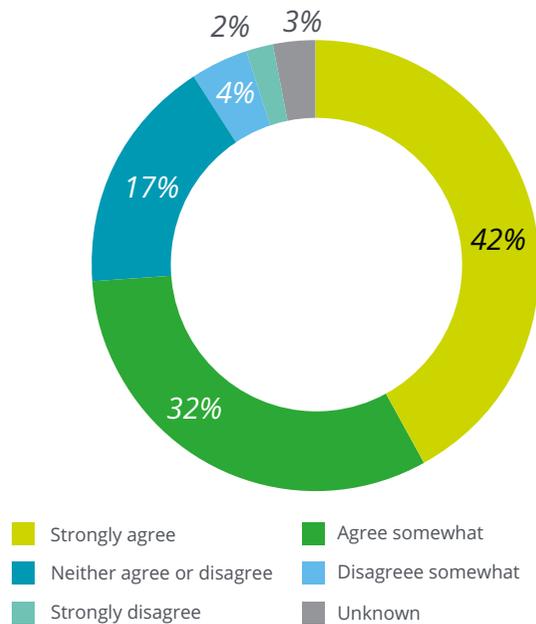


Fig. 11 Consumer concern about marketing cookies

Currently, **61%** of organisations mention cookie use in their privacy policy (including whether they are used for marketing or tracking purposes), but the consumer perception as outlined above suggests that this isn't enough. In fact, **95%** of organisations obtain consent for non-essential cookies through bundled consent received through the acceptance of a privacy policy.

"I am concerned about cookies that track my activity online and sell information about me to other companies"

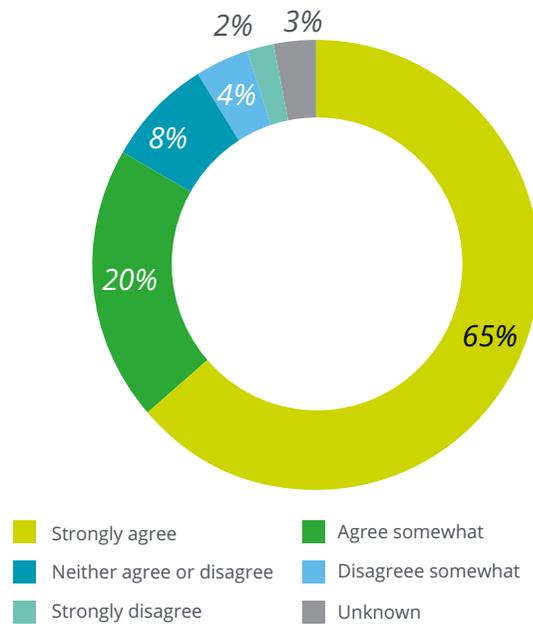


Fig. 12 Consumer concern about cookies that track online activity to sell to other companies

This suggests that consumers are unaware of when they have consented to have their online activity tracked for marketing purposes. In line with last year's Index, organisations need to do more to inform customers of the different ways that cookies are used and allow them greater choice and control in managing these cookies.

8.3 How is targeted advertising currently faring?

Using information collected through cookies, organisations can target customers with tailored ads, but when this practice feels invasive to people, it can prompt a strong backlash and a rejection of the advertising.

In fact, of the **74%** of consumers that raised concerns about how cookies were used to market to them; **82%** 'rarely' or 'never' buy something after receiving an online targeted ad. This demonstrates that consumers who are concerned about cookies that track their online activity also don't engage with targeted ads. Indeed, **65%** of consumers told us they are unhappy about receiving advertising targeted at them based on their online activity.

This current consumer sentiment is in stark contrast to the ubiquity of marketing cookies across the web. Our analysis showed that **98%** of brands have non-essential cookies on their websites and that each website contains, on average, **28** separate cookies which track a user's online activity for marketing purposes.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8**
- 9
- 10



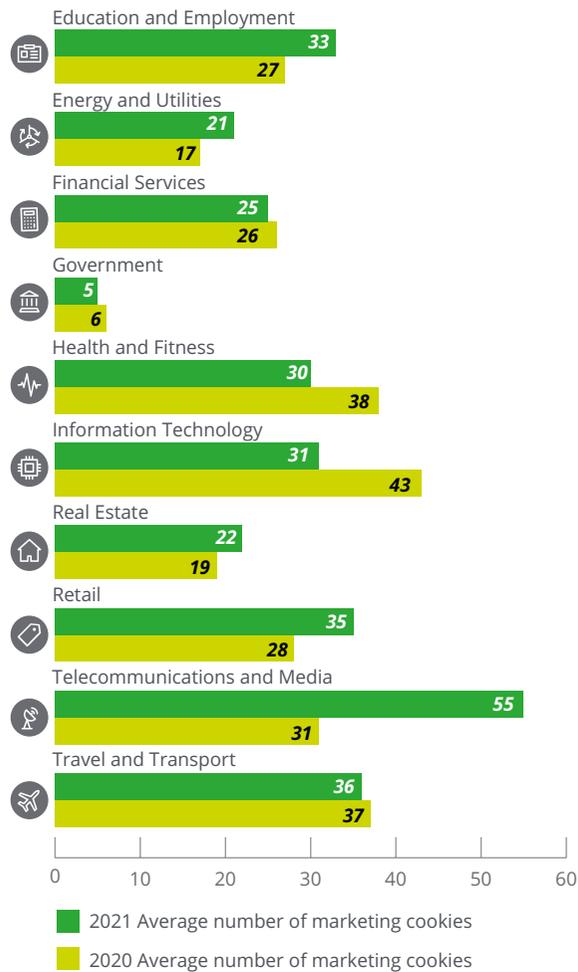


Fig. 13 Industry average of number of marketing cookies used

When comparing this year’s average number of marketing cookies across industry to the data collected last year, Telecommunication and Media are the only industry with a significant change. We have identified a **77%** increase in the average number of marketing cookies for this industry, growing from 31 in 2020 to 55 in 2021.

Ultimately, if companies continue with a business-as-usual approach and ignore consumer demand for greater web privacy, the effectiveness of targeted advertising is likely to decrease as consumer concern grows.

8.4 Current cookie management

The question then becomes, how can cookie practices be uplifted to better engage with customers? To answer this, the majority of consumers (**75%**) said they either currently manage their cookie preferences (**24%**) or want to manage their cookie preferences (**51%**). As a result, our research considered both how current cookie management tools can be improved, and what best practise in cookie management might look like in the future.

8.4.1 Consumers who manage their cookie preferences

Although **85%** of consumers are concerned about internet cookies that track their online activity and sell the data to other companies, only **24%** of consumers review their cookie preferences. These preferences can manage whether brands can track consumer activity online and use this information to market to them or sell their information to other companies.

The current process to update cookie preferences may not be as straightforward as required with **26%** of these consumers facing issues when updating their cookie preferences. One of the biggest complaints from consumers that had issues updating their cookie preferences was that the brand did not provide enough information on how to update their preferences and that any information provided by the brand was unclear and hard to follow. Another complaint that these consumers had was that the process to manage cookies was too time consuming or that they experienced some form of technical difficulty. On average, it took **10** clicks from landing on a website to being able to opt out of marketing cookies. This does not meet the expectations of global consumers, with **52%** expecting to be able to find what they need from a company in three clicks or less.⁴

These complaints align with the results from our brand analysis. Current information provided to consumers on how to update their cookie preferences is hard to find and unclear as **68%** of brands required consumers to navigate to their privacy policy to find out how to manage their cookie preferences. **29%** gave no instruction and only **4%** of companies had a cookie banner pop-up on the landing page which provided clear instructions or links to the privacy policy.

4. Salesforce, *State of the Connected Consumer Report*, 2019, p. 9.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10

How do brands instruct consumers on how to update their cookie preferences?

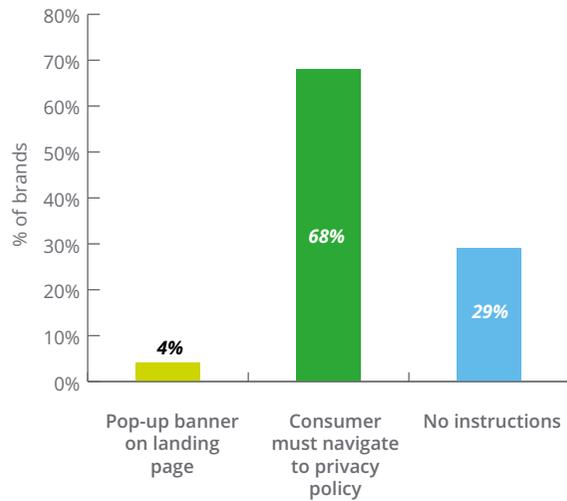


Fig. 14 How brands instruct consumers on how to update their cookie preferences.

Of those companies that did provide some information about updating cookie preferences, **88%** of brands instructed users to manage their cookie preferences in their browser. Consumers looking to change their preferences would then need to find out how to do this on the browser they use.

We conducted analysis over the most popular internet browsers to understand how easy it is for consumers to manage their cookies through these browsers. Most of those reviewed allow the choice between blocking all cookies, blocking third party cookies and allowing all cookies. Only one of the browsers reviewed offered an explanation as to the type of cookies that each setting would block (e.g. social media trackers and cross-site tracking cookies). Hence, for consumers to have greater control of their privacy rights, browsers should inform consumers exactly what types of cookies are blocked within each setting and allow consumers to block the specific types of cookies they don't want.

8.4.2 Consumers who don't manage their cookie preferences

Consumers have also made it clear that they want to manage their cookie preferences, even if they do not currently do so. In fact, **61%**⁵ of consumers who do not currently review their cookie preferences to manage whether brands track their activity have highlighted that they would nevertheless like to do so.

We asked these consumers how they would like to manage their preferences and the majority (**57%**) would like to set their preferences once, and for all brands to use those preferences.

How would consumers like to manage their cookie preferences?

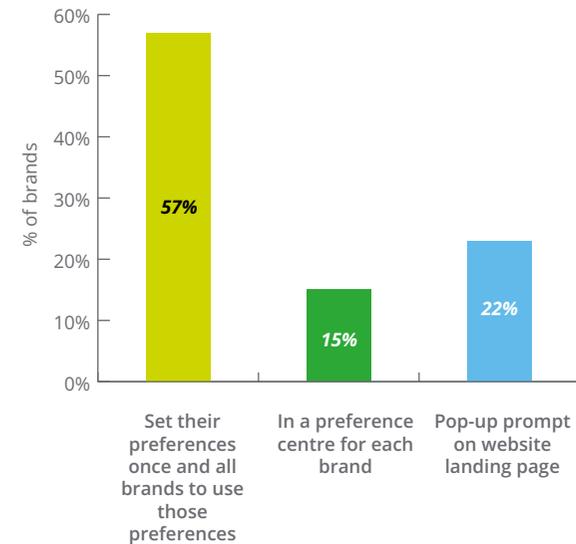


Fig. 15 How consumers would like to manage their cookies

Setting cookie preferences within a browser might meet this consumer desire of setting their preferences once. However, based on our brand and browser research it is clear that brands and browsers need to do more to clearly explain how consumers can set their preferences, what each preference choice means and enable consumers to get to these preferences in fewer clicks.

5. This equates to 51% of the total consumer population surveyed

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10

9. Methodology

9.1 The Index

The Deloitte Australian Privacy Index 2021 analysed the state of privacy, with a focus on the future of privacy in Australia. The Index reviewed Australia's leading consumer brands across 10 brand industries. The overall ranking of the Index was developed from:

- Analysis of the websites of 50 leading consumer brands active in the Australian market.
- Survey responses from more than 1,000 Australian consumers.
- The OAIC Notifiable Breach Scheme Reports (January – December 2020).
- OAIC Consumer Complaints Data.

9.2 Consumer survey

An external organisation, Roy Morgan Research, was engaged to survey the Australian consumers, to capture their opinions about the right to be forgotten, AI and targeted online advertising.

The survey was based on a nationally representative sample of Australian citizens and permanent residents aged 18 years and older. The sample was randomly drawn from the Roy Morgan Online Panel (RMOP). The RMOP consists of people who have been confirmed as being who they claim to be (i.e. they have not taken multiple membership of the panel and their demographic profile has been verified).

The RMOP currently consists of approximately 500,000 members aged 15+ and their profile closely reflects the demographic characteristics of the general population.

In total 1,006 questionnaires were completed. Quotas were applied to ensure that the distribution of the respondents was reflective of the overall Australian population aged 18 years or older in terms of location (State/Territory, Greater Capital City Statistical Area/Regional) age and gender.

Weighting was applied to the records using ABS population estimates for August 2020. This weighting re-distributed the survey estimates so that they represented the estimated population distribution, rather than the distribution of the sample. Similarly, the age and gender distribution of the sample was re-aligned to represent the current estimated proportion of age and gender in the various population groups examined in the Survey.

9.3 Brand analysis

We analysed 50 leading Australian consumer brands' websites according to a question set developed from topics raised in the Attorney General's Issue Paper for the review of the Privacy Act and based on responses received in the 2020 consumer survey. Inputs included each brand's privacy policy and consumer facing website. We also utilised a publicly available cookie scanning tool to test brands' websites for non-essential cookies.

This year we broadened our brand analysis to include a survey of some of our most prominent consumer serving clients to capture the brand perspective on the future of privacy in Australia.

In this Index we have not considered other online tracking technologies such as pixels.

1

2

3

4

5

6

7

8

9

10



10. References

10.1 National

- *Privacy Act 1988* (Cth).
- ACCC Digital Platforms Inquiry Report – June 2019
- The OAIC Notifiable Breach Scheme Reports (January – December 2020)
- The OAIC Annual Report 2020
- OAIC submission in response to the Attorney General's Issues Paper, December 2020
- Deloitte, (2019) [Conversational AI: Conversational AI is powering the next wave of customer and employee experiences](#)
- Salesforce, (2019), [State of the Connected Consumer Report](#)

10.2 International

- *General Data Protection Regulation 2016/679* (EU)
- Regulatory Guidelines and Reports
- EU ePrivacy Directive



1

2

3

4

5

6

7

8

9

10



Contacts



Daniella Kafouris

Partner | Risk Advisory | Melbourne
dakafouris@deloitte.com.au



Tom Rayner

Partner | Risk Advisory | Perth
trayner@deloitte.com.au



Rachelle Koster

Partner | Risk Advisory | Canberra
rkoster@deloitte.com.au



Tommy Viljoen

Partner | Risk Advisory | Sydney
tfviljoen@deloitte.com.au



David Hobbis

Partner | Risk Advisory | Adelaide
dhobbis@deloitte.com.au



Judith Donovan

Partner | Risk Advisory | Brisbane
JDonovan@deloitte.com.au



Elizabeth Lovett

Partner | Risk Advisory | Hobart
ellovett@deloitte.com.au

About the team

The Privacy experts in our Cyber Risk Practice who developed the Deloitte Australian Privacy Index 2021 included:

- Celia Cavanagh, Project Manager;
- Sara Baroudi, Project Co-ordinator;
- Piya Shedden, Project Reviewer;
- Marie Chami, Project reviewer;
- Paul Casey, Project Writer;
- Meg Linke, Project Writer;
- Joshua Cutrone, Project Writer and Researcher;
- Katherine Fan, Project Writer and Researcher;
- Yianni Anastasiadis, Project Writer and Researcher

1

2

3

4

5

6

7

8

9

10





This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organisation”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 286,000 people make an impact that matters at www.deloitte.com.

Deloitte Asia Pacific

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities provide services in Australia, Brunei Darussalam, Cambodia, East Timor, Federated States of Micronesia, Guam, Indonesia, Japan, Laos, Malaysia, Mongolia, Myanmar, New Zealand, Palau, Papua New Guinea, Singapore, Thailand, The Marshall Islands, The Northern Mariana Islands, The People’s Republic of China (incl. Hong Kong SAR and Macau SAR), The Philippines and Vietnam, in each of which operations are conducted by separate and independent legal entities.

Deloitte Australia

In Australia, the Deloitte Network member is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia’s leading professional services firms. Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 8000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at <https://www2.deloitte.com/au/en.html>.

Liability limited by a scheme approved under Professional Standards Legislation.
Member of Deloitte Asia Pacific Limited and the Deloitte Network.