Deloitte.

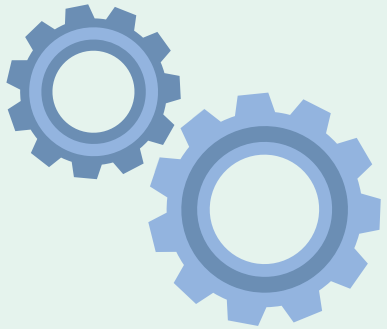
Opting-in to meaningful consent

Deloitte Australian Privacy Index 2020

Contents

"The practical application of concepts of fairness and the role of consent will be central to the future of privacy in Australia."

OAIC Submission to the ACCC Digital Platforms Inquiry, May 2019



1 Introduction

2 About the report

3 Key findings

4 Top takeaways for better consent

5 Privacy Index 2020

6 Consumer sentiment analysis

7 Brand analysis

8 Methodology

9 References

10 Contacts

Introduction

It's been another big year for privacy. All that's happened in the last 12 months has us edging ever closer to some significant regulatory and social change in this space.

Two years from the Cambridge Analytica scandal we're still seeing its effects, from the ACCC's 2019 Digital Platforms Inquiry, which the Government indicated in late 2019 would lead to regulatory change, to the landmark case the Office of the Australian Information Commissioner (OAIC) has brought against Facebook in the Federal Court.

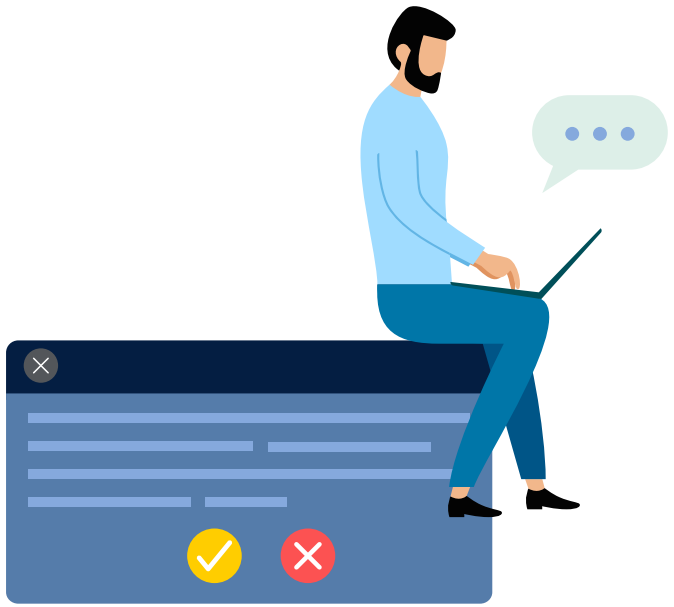
In addition, 2020 is showing us how privacy is central to building trust as we continue to find our way through the first global pandemic of the digital age. COVID-19 has put pressure on governments and enterprises to use technology with the data they have – or can collect – to protect us and our economy. Meaningful consent should now be front and centre for every industry and every sector. To that end, good consent has certain qualities, which is explored in detail in this Report. Australians have also overwhelming told us that they don't like being marketed to without opting in, or bundled consent which couples something we do want with something we don't, especially when it is unnecessary.

The key is in empowering people to choose if and how they participate. We're seeing this in COVID-19 initiatives such as tracing apps, where the concept of care drives voluntary participation and builds trust between community and government. It has also allowed the government to send a clear message to enterprises and brands; you can maintain privacy at the same time as furthering important social and economic objectives.

To prosper as a society, we should foster innovation and embrace change, but not without due consideration of one of our fundamental human rights: privacy. Our previous Privacy Indexes have shown that consumers are likely to forgive a brand for something like a data breach, but they are extremely unforgiving of conscious acts such as the sale or disclosure of their data to third parties, which are not necessary for or related to the service we seek. If we're to maintain trust in institutions and corporations, meaningful consent is essential. Now the community is waking up to the power and value of data, real transparency, fair value exchange and true voluntariness will be required to establish consent and trust.

In 2019, the Chief Data Officer at one of Australia's leading banks asked Deloitte 'What does good consent look like, and who's doing it well?' After considering this for a while our team realised these great questions weren't easy to answer in an evidence-based way. We had our opinions and knew the theory, law and regulatory guidelines, but we didn't have any research that pondered these questions in depth. That's why this year's Index theme is focused on consent. We have examined the behaviours of the top 100 brands in Australia where they operate using 'consent' as the basis for processing personal information. We have then compared this behaviour against what 1,000 Australians told us constitutes meaningful consent to them. Of course, what constitutes meaningful consent and permission will be different to every person and our research shows that, but it overwhelmingly shows a disconnect between what consumers expect and what brands are actually doing to gain their consent.

Meaningful consent is the real opportunity in COVID-19 times and beyond. It is the responsibility of every organisation in Australia processing personal information to do its bit in increasing trust in the digital economy. As we build trust and access the social licence that comes with it, we will be better placed to unleash the remarkable opportunities and innovations rich data brings.



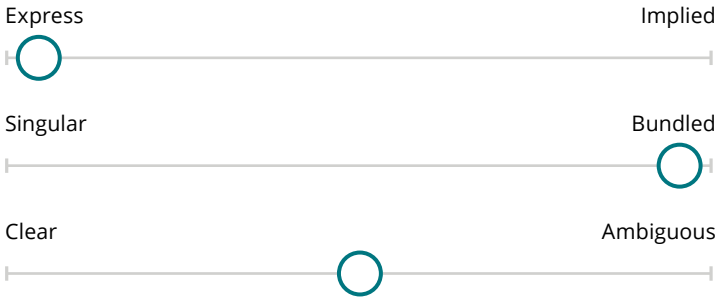
About the report

Under the Privacy Act, organisations are required to collect consent from consumers prior to certain processing of their personal information. The OAIC has published guidelines on what good consent looks like. Consumers have told us where their expectations lie when giving brands consent to collect and process their personal information.

Introduction to consent

Consent can be either **expressly given or implied**, where express consent is collected through affirmative actions and implied consent through passive actions, e.g. pre-ticked boxes. Consents can be **collected singularly** for each processing activity, e.g. separately collected consent for a service and for marketing activities, **or bundled together**, e.g. consent to an entire privacy policy. Consent can be communicated to the consumer in a **clear or ambiguous manner** where clear consent is best practice. However, ambiguous consent is commonly seen and can involve masking the reason for consent within legalese and lengthy terms and conditions. We have observed brands using a combination of these dimensions in their own consent practices; one might use an affirmative action (express) to collect consent but have all consents bundled together through acceptance of the privacy policy. It is noted that bundled consent is not necessarily a bad approach; the issue arises when consent for the primary purpose is bundled with consent for other non-essential purposes such as marketing and tracking.

Consent variation example



In this Privacy Index we often refer to consent best practice and by that we mean meaningful consent: consent that is voluntary, informed, expressly given, specific as to purpose, time-limited and able to be easily withdrawn. Having said this, and understanding the challenges we face within existing legal and technical constructs, not all consents to process can practically and realistically be delivered in the best practice format. Australians have told us when they expect the higher bar for consent, and when they don't. Typically speaking, the more sensitive the information being processed, and the more intrusive the processing, consumers have told us that the 'higher bar' will be more meaningful to them.

Consumer sentiment analysis

In this 2020 Deloitte Australian Privacy Index we surveyed more than 1000 Australian consumers aged 18 and above asking them about their personal consent-giving practices when interacting with apps and websites.

We also asked:

- How privacy considerations impacts their decision to interact with a technology and brand.
- Which brands they trusted the most and least when it comes to good privacy practice.

To understand how consumers feel about consent-giving in the website and mobile app environments, we also asked:

- Whether they have concerns about their consent for a service being used for other purposes that are non-essential for delivering that service.
- Whether they feel overburdened by the number of consents that are requested from them.
- Whether the number of consents requested impacts their decision to read specific terms and conditions.

Brand analysis

We investigated the websites and mobile applications of Australia's top 100 consumer brands, examining the consent behaviours and attributes of those websites and apps. We focused on the type of consent and the point in the consumer journey at which the consent is collected; whether that be explicitly given by the consumer, implied by the actions of the consumer or not collected at all. These results have been aggregated across the industry sectors within which each brand operates to provide an industry sector specific view on consent.

The Index

This year we analysed brands by assessing the consent practices of their websites and mobile apps. We tested each website and app against consent best practices as well as comparing the results between the websites and applications to test for consistency. We combined the findings of the brand analysis with selected findings from the consumer survey, as well as sector level breach and complaints data published by the OAIC. The results were scored and aggregated across 10 industry types enabling us to rank each industry to create the Index.

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.

Acknowledgments

We would like to acknowledge the following for their support:

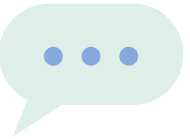
- Roy Morgan Research Ltd for conducting the consumer survey on behalf of Deloitte.
- The participants of the consumer survey for providing their responses.

Key findings

This year's Privacy Index highlights the vast difference between consumer expectations and industry consent practices. Across industry we have seen a lack of maturity in the consent space, such that any updates to Australian law would require significant industry changes and uplift.

Only 16% of brands offered consumers the option to opt-in to marketing activities, while **64%** obtained this consent through the bundled acceptance of their privacy policy. Of these 64%, **65%** limited the functionality of the website without obtaining this consent, meaning consumers have little choice but to consent to marketing activities.

Only 21% of brands provided consumers with a comprehensive consent management portal or equivalent that was also fully or partially available from the associated application.



50% of consumers stated that they had given consent (when they had previously refused) because they were tired of being asked continuously by the same service.

Only 7% of consumers said they had a very good understanding of how their personal information would be used after they consented to its use.

None of the top 100 consumer brands met consent best practices for cookie management.

52% of brands obtained consent for non-essential cookies through the bundled consent of accepting a Privacy Policy.

Only 12% of consumers thought consent given for non-essential uses should be enduring.

7% of the brands that did not mention marketing activities in their privacy policy were found to use marketing cookies when their website was tested.

Only 33% of consumers agreed that their consent for non-essential processing is valid when it is obtained through acceptance of the terms and conditions and/or privacy policy.

83% of consumers said they are concerned by internet cookies that track their activity online and use this information for marketing purposes or to sell information on to third parties.

Top takeaways for better consent

Gaining meaningful consent from consumers, within current legal and technical constraints, isn't easy. Striking the balance between the optimal user experience and obtaining meaningful consent differs across platforms and use cases.

No one wants to give consent through endless pop-ups, nor do they consider consent meaningful when it's driven through catch-all, non-specific privacy notices. There is an opportunity for brands to increase their operational efficiency, increase transparency and grow consumer trust by getting their consent practices right. Some key actions to help achieve this are:

1

Have a smart consent strategy

Decide whether you want to follow the minimal legal approach to gaining consent, or whether you want to position your brand as a data ethics leader by following best practices.

2

Understand your data

For most businesses, the single biggest hurdle to operationalising consent management is foundational data governance, and data management practices and capabilities. These can enable you to follow personal information from the moment it's collected to its destruction. How can you manage consent if you don't know where the personal information you process is, where it came from and what permissions you have in relation to it?

3

Don't bundle certain consents

Consumers have clearly indicated a strong preference to opt-in to certain activities that aren't essential for the service they seek, such as marketing, online tracking and some physical location tracking. To meet this consumer preference, you should not bundle the consents required for providing the service with those that are not. Ask for express permission to do these things at the appropriate time in a way that is as 'frictionless' as possible.

4

Create an online portal for users

Provide a digital portal for consumers to monitor and change their consents. Make it easy to access, understand and use. This can increase transparency, individual control and trust – enabling you to demonstrate how you take consent seriously.

5

Give granular cookie choices

Give more than two choices in your cookie consent banners and avoid the all or nothing approach. Allow consumers to opt-in to tracking and marketing cookies and don't have this turned on by default or bundle the consent with other functional, less invasive cookies.

Privacy Index 2020

How each sector ranked

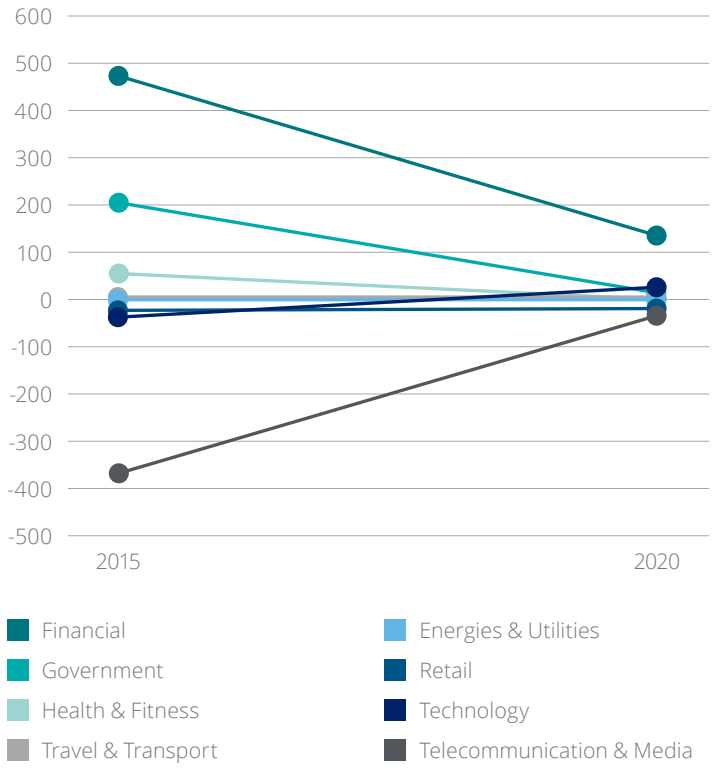
	Current ranking	Previous rankings		
Index Focus	**Consent**	Apps	Notice	Data Protection
Year	**2020**	2019	2018	2017
Retail	1	5	7	10
Government	2	8	2	2
Information Technology	3	1	9	7
Travel & Transport	4	3	N/A	8
Real Estate	5	2	8	13
Education & Employment	6	6	11	6
Energy & Utilities	7	4	4	3
Telecommunication & Media	8	7	3	N/A
Finance	9	9	1	1
Health & Fitness	10	10	6	4

Overall Index

Each year the Privacy Index focuses on a different privacy element and as such should not be treated as a like for like comparison. Rather it should be viewed to create a holistic view of each industry's privacy posture across each of the focus areas from previous Index editions. For example, the Information Technology sector has leading application privacy (as of 2019) but performed poorly in providing notice to consumers about the uses of their personal information (as of 2018).

By focusing on consent practices in the 2020 Privacy Index, the sector rankings have shifted. Retail has jumped from 5th to 1st position demonstrating that, as an industry, they manage consent privacy practices (as of 2020) better than those to do with applications (as of 2019). However, this does not indicate that even Retail provides consent best practices to consumers. Our industry analysis found that no industry scored above 30% when we tested their consent practices, demonstrating the industry wide immaturity in this space.

Trust in privacy six years on



Each year we ask over 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. A score of 0 on the graph represents as many trusting as distrusting consumers. It's important to note that we also consider leading government service delivery brands in this survey.

From our first Index in 2015 to now, there has been some significant movement in the consumer trust in privacy scores. Financial services have seen the biggest loss in trust in privacy, but are still in positive territory, meaning more consumers trust than distrust financial services brands with their personal information. Government has also had a significant drop in trust in privacy over this period, returning a near zero result in 2020, meaning there were as many consumers saying they trusted Government brands as there were distrusted.

The Telecommunications and Media sector continues to retain its position as least trusted by consumers overall, albeit on a positive trajectory. 94% of consumers that distrust this industry named Social Media brands as those they trusted least. This is not a surprising result given the high-profile data breaches across social media brands in recent years, as well as social media brands' involvement with broader privacy breaches e.g. data scraping. It's important to note that this does significantly impact the Telecommunications and Media sector as a whole.

Consumer sentiment analysis

We surveyed more than a thousand Australian consumers asking them about their personal consent practices when interacting with mobile apps and websites of brands.

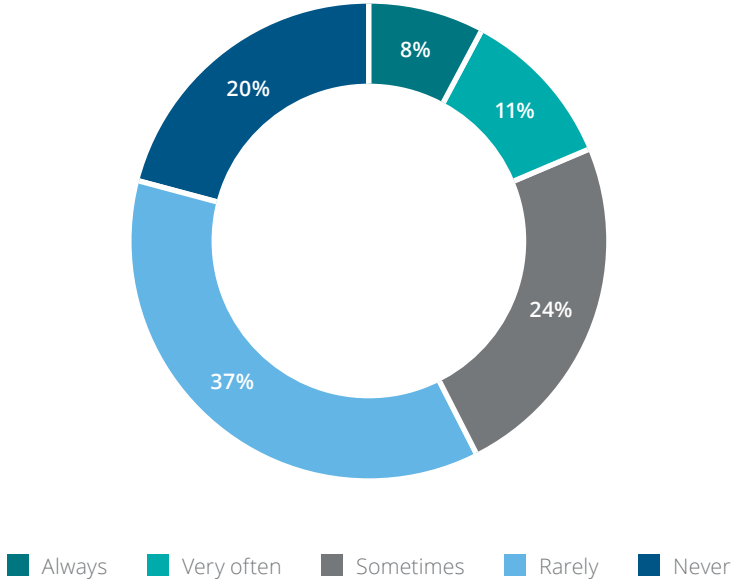
Before giving consent

In the current climate, consumers are being asked to provide more personal information than ever before, and organisations are asking for their consent as a way of legitimising this additional processing of personal information. We asked questions of consumers to understand how they feel about this type of consent collection and how the capacity of consumers should be considered when collecting consent.

Consumer engagement in consent collection

Consumer engagement with brands' privacy policies has reduced over the last year, which does not reflect the increasing concerns consumers have shown in relation to their privacy, meaning brands could do more to engage with their consumers. In the 2019 Privacy Index, 68% of consumers indicated that at some time they had read at least part of a privacy policy before deciding to download a mobile app. This year, only 43% of consumers indicated that they would at least "Sometimes" read the terms and conditions or privacy policy before giving consent to a service.

When signing up for a service online how often do you read the terms and conditions or privacy policy online before signing up?



Sixty-four percent of consumers agreed that they felt overburdened by requests for consent when signing up to a service and almost 80% of these consumers stated that feeling overburdened makes them less likely to read the privacy policy and terms and conditions associated with these requests before giving their consent. 50% of overburdened consumers indicated that they had given consent (when they had previously refused) because they were tired of being asked for consent continuously by the same service. This provides evidence to suggest significant consent fatigue amongst consumers.

Only 7% of consumers responded by saying they had a very good understanding of how their personal information would be used after they provided their consent. 71% of consumers indicated that they did not fully understand the use of their personal information, including 15% of consumers who did not have any idea what they were consenting to.

This calls into question the validity of the consent collected by organisations currently. OAIC guidelines require organisations to ensure that an individual is properly and clearly informed about how their information will be handled in order to provide consent. If approximately half of consumers are consenting for ease of use and over half of consumers do not fully understand what they are consenting to, how informed can the consumer be, to be able to provide informed consent? In addition to this, how can brands depend on, and manage, this consent for their day to day operations if it does not meet these OAIC guidelines?

Age considerations

While age considerations do not have the force of law yet in Australia, our research found that consumer expectations largely align with the consent requirements of the European regulations, as 73% of consumers stated that they did not think children under the age of 16 should be allowed to consent to the processing of their personal data online.

"Where the personal information of children is collected, consents to collect the personal information of children must be obtained from the child's guardian."

ACCC Digital Platforms Inquiry report

Choice and control

Consumers appear to be expecting a greater degree of control and choice over how organisations use and disclose their personal information. As we will discover in the Brand Analysis section of this report, many industries continue to bundle consent for their primary offering with that of non-essential uses, such as marketing, tracking and certain disclosures to third parties. We asked consumers about their opinions on the degree of transparency, choice and control they have been provided with. This is specifically regarding the processing of their personal information that is not essential for the completion of the service they are consenting to, how they manage their consent for cookies, and whether they have considered revoking their consent based on privacy concerns.

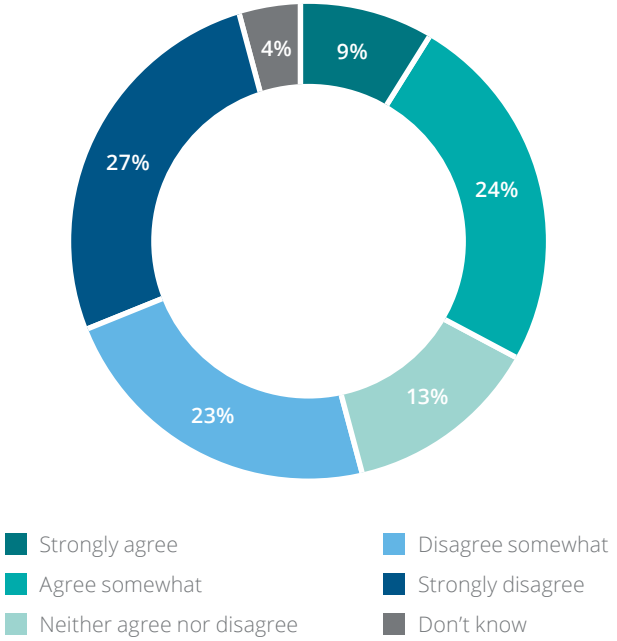
Non-essential processing

From our brand analysis, we found that organisations are most often using bare minimum consent practices to obtain consent digitally from individuals to put data to uses that are not related or not essential to the service or offering a consumer is seeking. This involves:

- Bundled consent – in the case where the bundle contains consent for non-essential processing such as marketing and tracking activities.
- Click-wrap agreements – these are online agreements using digital prompts that request users to provide their consent to online terms and policies without requiring them to fully engage with the terms and policies of use.
- Take-it-or-leave-it terms – these are terms and conditions which do not provide consumers with enough detail, information, choice, control, or power to make decisions about the use of their personal information.

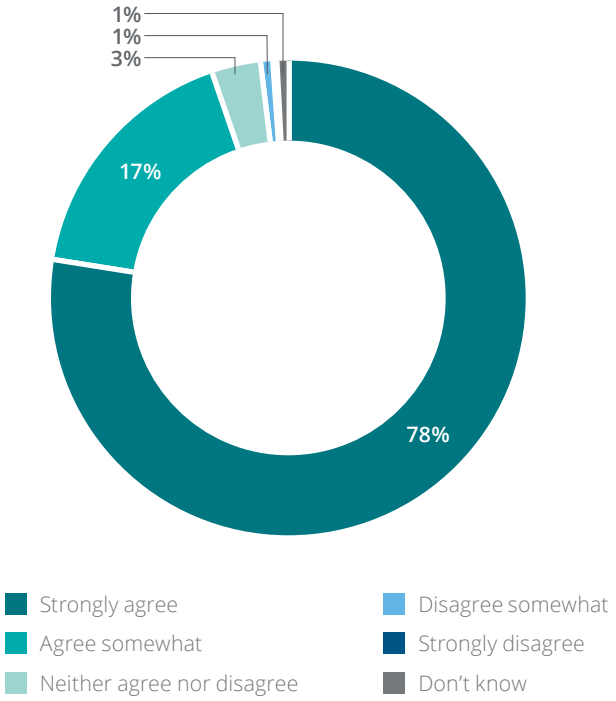
Only 37% of consumers agree that they have provided an organisation with valid consent for non-essential processing when that processing was mentioned by the terms and conditions and/or privacy policy.

When the terms and conditions and privacy policy are available to read and mention that they will use your personal information for non-essential purposes, do you agree or disagree that you have given valid consent for those uses of your personal info?

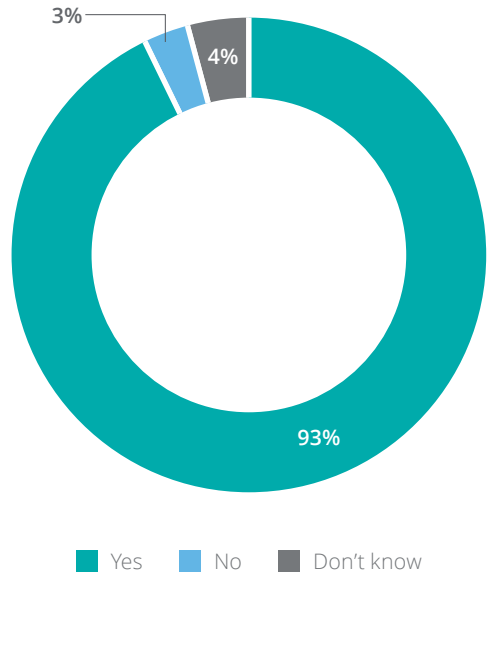


To address these practices, 95% of consumers agree that terms and conditions should clearly state that an individual can quickly and easily opt-out of allowing the service access to their personal information for unrelated purposes. 93% of consumers agree that they expect a service to provide them with the option, upfront, to opt-in to non-essential uses of their personal information rather than having to opt-out of these uses.

Before I decide to sign up to a service, the terms and conditions online should clearly state that I can quickly and easily opt-out of allowing the service access to my personal information for unrelated purposes.



Do you expect a service to give you the option, upfront, of opting in to non-essential uses of your information such as marketing and sharing your personal information with other organisations?



"There is a substantial disconnect between how consumers think their data should be treated and how it is actually treated."

ACCC Digital Platforms Inquiry report

Our findings highlight the significant imbalance that exists between current organisational practices and consumer expectations.

Organisations could use this as an opportunity to improve the quality of their marketing databases by aligning with consumer expectations for privacy. When strong consent practices are in place, such as opt-in, organisations could significantly improve the quality of the consent held and avoid adverse effects when marketing activities delivered to consumers who have not asked for them. Such privacy practices should be viewed as a business enabler, not an inhibitor.

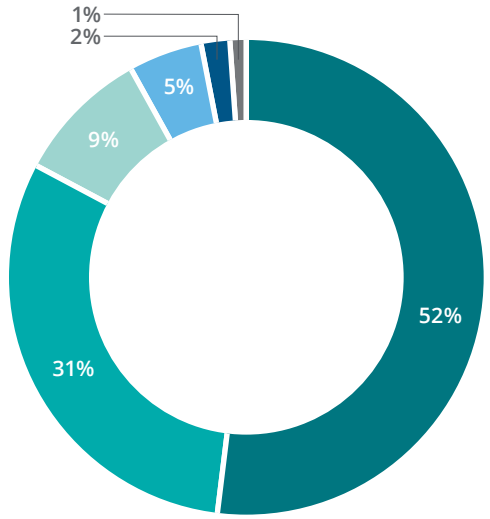
Cookie management

Our findings show that consumers continue to be concerned by online tracking through cookies. Cookies can be, and are, used to track consumer activity, and to conduct targeted marketing and advertising. However, the current approach used by organisations (website banners, terms and conditions, privacy policies, and cookie statements) to keep consumers informed of the uses of their personal information, rights and ability to manage cookies could be closely associated with consent fatigue and overall lack of engagement.

Eighty-three percent of consumers said they are concerned by internet cookies that track their activity online and use this information for targeted marketing purposes or to sell their information to other companies. This suggests that consumers care about the way organisations use this information. It also suggests organisations could improve the way consumers are informed about the use of cookies, and ultimately to rework the way consent is obtained from individuals.

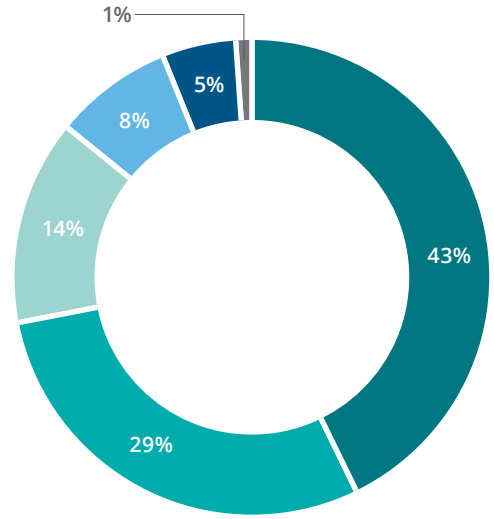
However, 72% of respondents are annoyed by the banners contained on websites, which ask them to agree to the use of cookies. This suggests that these banners do not provide adequate or user-friendly information and options for consumers to alleviate concerns, particularly for the purposes of collecting data to track online activity and behaviour. This also demonstrates the challenge facing brands in communicating their cookie practices to their consumers, as nearly three quarters of consumers are annoyed by cookie banners on websites.

I am concerned about internet cookies that track my activity online and use this information to market to me or sell information about me to other companies.



Strongly agree
Agree somewhat
Neither agree nor disagree
Disagree somewhat
Strongly disagree
Don't know

I am annoyed by the banners on websites which ask me to accept cookies.



Strongly agree
Agree somewhat
Neither agree nor disagree
Disagree somewhat
Strongly disagree
Don't know

Revoking consent

We consider the ability to revoke consent a key factor in consumer choice and control.

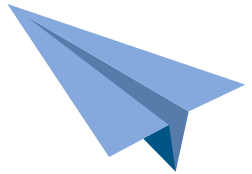
Sixty-six percent of respondents confirmed that they had backed out of purchasing a product or using a service, or closed an account completely, due to privacy concerns in the past. Roughly 50% had done this between 2 and 5 times in the past 12 months.

When asked why they would decide not to provide their personal information, consumers responded that the main reasons were that they did not agree with some of the uses of their personal information (46% of responders) or with the T&C's more broadly (44% of responders).

This illustrates the significant value consumers are placing on their privacy, with consumers choosing to provide consent to organisations with privacy ethics that align to their own. Organisations that adopt pro-consumer defaults through singular and express consent should be able to differentiate themselves in the market, likely expanding their commercial presence.

"The more value you offer, the more comfortable consumers will be with sharing their data."

Deloitte Meaningful Brands, 2018



Maintaining consent

We asked our survey participants how and when they wanted to have their consent renewed.

Only 12% of consumers think that giving consent once is enough for its use for non essential purposes and only 8% of respondents want their consent to be refreshed on a periodic basis of every 12 months. This suggests most consumers want to have more control over the consent they give (88%) but are resistant to being required to refresh their consent at regular defined time intervals.

When we break this data down further by age of participant, we uncover some additional trends.

	18-24	25-34	35-49	50-64	65+
Never, once is enough	6%	7%	9%	15%	21%
When there is a change	45%	36%	31%	23%	20%
Every 12 Months	8%	10%	9%	6%	6%
Every time the PI is used	38%	47%	51%	56%	52%
Other	2%	2%	0%	0%	0%

Of the 12% of people who said they think it's enough to collect consent once, 67% of them were over the age of 50, with only 6.5% of 18-34-year-olds responding that providing consent once is enough. Our older responders were also more likely to state that consent should be requested each time their personal information is to be used for an unrelated purpose, in line with a historical (and current Australian) view of consent.

Of the younger participants (18-24) the most popular response was that consent should be requested whenever there is a change in how their personal information is used. This is much more aligned to the European approach to consent under the General Data Protection Regulation (GDPR), which requires consumer consent to be tied to specific purposes, such that any additional purpose requires additional consent. Consumers are increasingly coming to expect this level of consent as they interact with global brands that are required to follow the GDPR consent requirements within Australia. This supports the Digital Platforms Enquiry that recommended Australian law around consent be updated, which would bring it in line with consumer expectations.

Brand analysis

The misuse of personal information continues to hit headlines. Locally and globally, new and updated privacy laws are being considered, developed, and implemented.

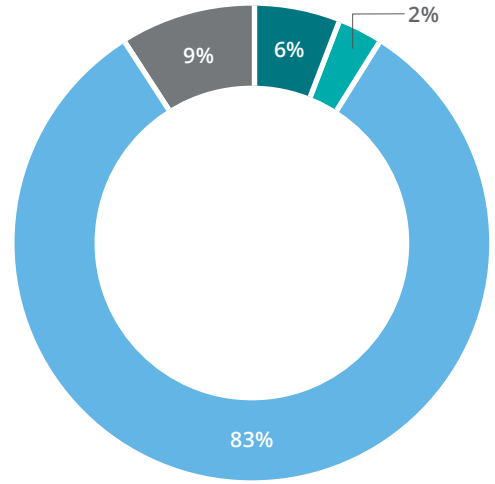
Cookie consent

We assessed the top 100 consumer brands against consent best practices, which include obtaining express, singular and clear consent from consumers for non-essential cookie types (e.g. marketing and tracking cookies) before dropping them onto consumer devices. However, our brand analysis found that none of the top 100 consumer brands met this standard of cookie consent.

We found that 83% of brands are not informing consumers about the non-essential cookies they are using, calling into question the transparency of this processing. This aligns with the consumer analysis finding that 83% of consumers said they are concerned about internet cookies that track their activity online, suggesting that brands could alleviate some of these concerns by sufficiently informing their consumers. These brands could be assuming the consumer's consent is provided by and upon accessing the organisation's website, including acceptance of hidden, lengthy and sometimes legalistic terms and conditions, and privacy policies.

The full breakdown of marketing and tracking cookie consent approaches across the brands is as follows:

Does the brand's website deploy marketing or tracking cookies?



- Yes – Has a cookie banner or equivalent on first visit that remembers your preferences for subsequent visits
- Yes – Has a cookie banner or equivalent on first visit that doesn't remember your preferences for subsequent visits and is deployed every time
- Yes – Not have a cookie consent banner or equivalent cookie consent collector
- No – According to the brand's privacy policy the website does not deploy marketing or tracking cookies

Surprisingly, 7 of the brands that do not mention marketing activities in their privacy policy were found to use marketing cookies when their website was tested.

Using a publicly available tool we found that the average numbers of marketing cookies dropped onto a user's device when visiting brands websites per sector are:

Industry	Average marketing cookies
Education & Employment	27
Energy & Utilities	17
Financial	26
Government	6
Health & Fitness	38
Information Technology	43
Real Estate	19
Retail	28
Telecommunication & Media	31
Travel & Transport	37

The average number of marketing cookies is lowest for Government and highest for Information Technology consumer brands. Finance brands were named by consumers as their most trusted brands ('Overall Index' section); these consumers may be surprised at the relatively high number of marketing cookies used across this industry.

While signing up to a brand

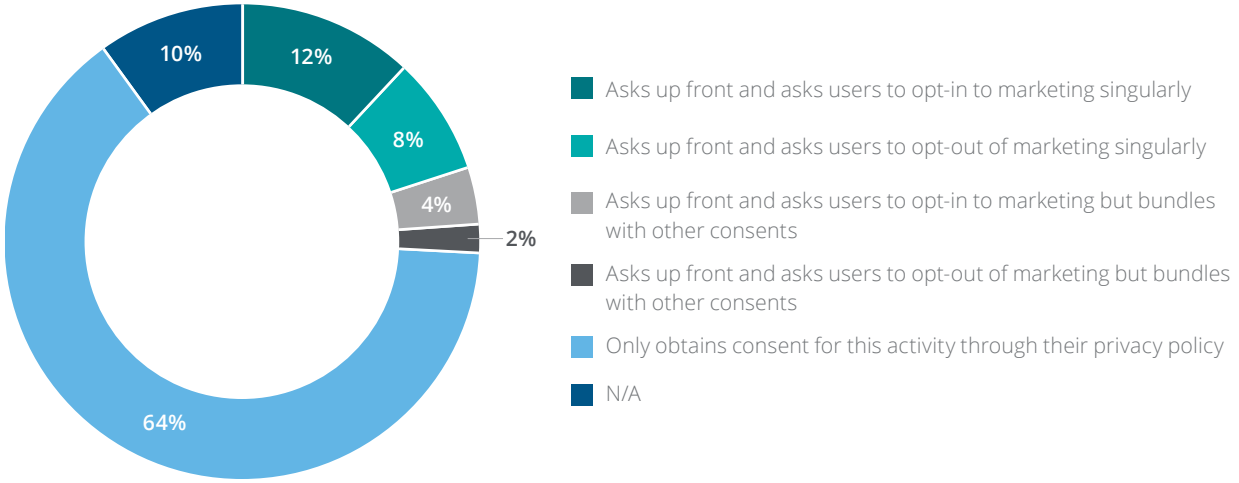
We found that the sign-up process is typically the point where brands start to collect significant amounts of personal information from a consumer.

Our research showed that 70% of brands bundle consent and only 20% of brands request for singular consent for certain types of personal information processing activities. 52% of the brands bundle consent in the Privacy Policy where non-essential activities were included. In 81% of cases the brand explains what the consumer gets in return for providing their consent, such as receiving a specific service. All the researched brands in the Information Technology industry explain what the consumer receives in return for providing their personal information. However, 50% of those brands provide the explanation through their privacy policies.

Forty-six percent of the brands explicitly state that they will not process personal information for any other purposes than those set out in their privacy policies. 78% of the brands in the Government sector listed use cases where they would not process personal information. This is the highest percentage across all the industries.

Personal information will be processed for a variety of reasons, including marketing activities. Our research has found only 16% of the brands ask consumers to opt-into marketing activities. The majority (64%) of brands mention marketing activities in their privacy policy but do not inform consumers that they can opt-in or opt-out of marketing activities separately. In this case, consent for marketing activities has been bundled with other processing activities when accepting the privacy policy. Our research shows the retail industry scores the highest relative to the other industries with 61% of brands within that industry obtaining explicit consent for marketing activities prior to a consumer signing up for their service.

Does the brand say in their privacy policy that they will be using the personal information they collect for marketing? Does that brand then ask for consent for that activity?



While using a service

Most brands researched require consumers to sign up with their personal information to access a service and/or purchase goods. Of the brands that provide a service where signing up should not be essential (as opposed, for example, to subscription services, banking and finance and where true identity is required etc.) only 11% gave complete access to the service without first requiring consumer consent through a sign-up process. Where consent is not provided there is a limited functionality for 63% of the tested websites, and 36% of the tested apps are completely inaccessible without signing up to the service. This suggests the consent to process personal information for non-essential activities loses its meaningfulness as it's hard to argue that it's been given voluntarily.

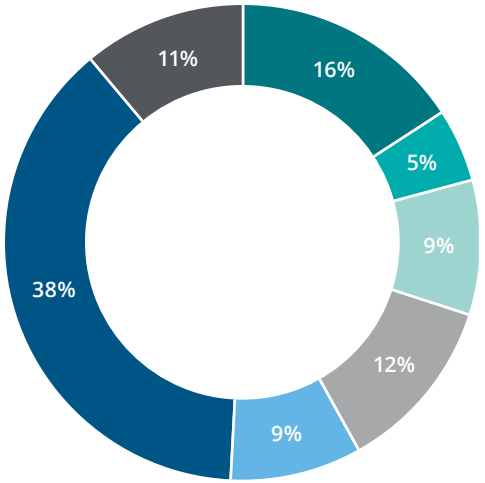
Once an individual has provided consent, it's best practice for organisations to provide consumers with the option to manage their preferences. For example, by providing or revoking consent for specific uses. This is commonly undertaken via a consent management portal or preference centre.

We found that 38% of brands tested did not provide their consumers with a self-manageable, easy and readily accessible option to manage their consent for the handling of personal information, potentially reducing the meaningfulness of consent provided over a period of time.

Fifty-three percent of brands tested do have a preference centre or consent management portal available to consumers. However, only 16% of brands provide their consumers with a comprehensive preference centre where it is accessible from all major platforms used to interact with consumers, predominantly being a mobile website, full web browser and mobile application.

Our research found that 67% of the brands within the Information Technology sector and 62% of the brands in the Retail sector offered a comprehensive privacy portal on their website or mobile application to manage their consents.

Does the brand have a preference centre or consent management portal?



- Yes – It is comprehensive and I can give or revoke all the relevant consents for that product/service in the one place in real-time – and it's accessible from their mobile website/app as well as the full version of the website
- Yes – It is comprehensive and I can give or revoke all the relevant consents for that product/service in the one place in real-time – and it's partly accessible from their mobile website/app as but fully available from the full version of the website
- Yes – It is comprehensive and I can give or revoke all the relevant consents for that product/service in the one place in real-time – it's not accessible from their mobile website/app as but fully available from the full version of the website
- Yes – Covers some of the consents that would need to be considered by that brand but not all the areas that should be covered, and it this is fully available from both the mobile website/app as well as the full version of the website
- Yes – Covers some of the consents that would need to be considered by that brand but not all the areas that should be covered, but this is not available from the mobile website/app, but available from the full version of the website
- No – The brand does not have a place to manage consents
- N/A

Industry ranking for nature of consent management portal offered to consumers

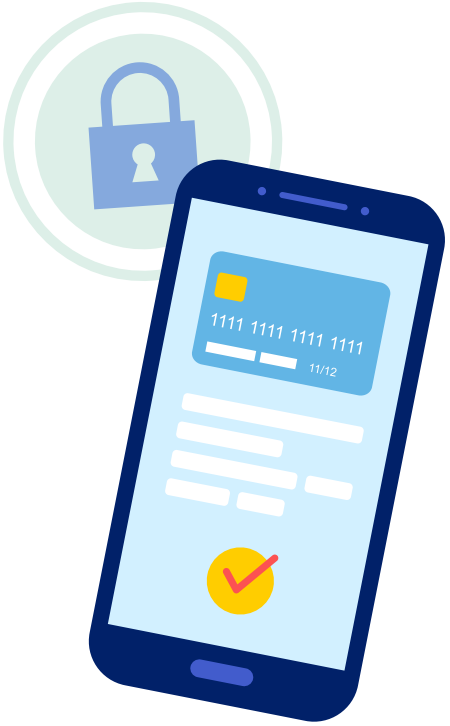
Industry	Testing Rank
Information Technology	1
Retail	2
Real Estate	3
Telecommunications & Media	4
Travel & Transport	5
Financial	6
Education & Employment	7
Government	8
Energy & Utilities	9
Health & Fitness	10

Comparison between brand's website and mobile application

In testing the top 100 consumer brands we looked at both the brand's website and their mobile application. The results for these were largely comparable. However, there was one noticeable exception. Across industry 72% of tested websites allowed full or partial functionality without consent, whereas only 38% of tested apps allow full or partial functionality without consent. This could be due to the websites providing information as well as subscription services. However, the apps were found to be more targeted at consumers who have already signed up for subscription services, hence requiring a log-in credential (and associated consents) to access.

"Organisations that shift to using new mediums for doing business need to replicate, as far as possible, privacy and security measures that would apply in their regular environment."

Angelene Falk, Australian Information Commissioner and Privacy Commissioner



Methodology

Findings

The Deloitte Australian Privacy Index 2020 analysed the state of privacy, with a focus on consent, of Australia's leading consumer brands across 10 brand sectors. The overall ranking of the Index was developed from:

- Analysis of the websites and mobile apps of 100 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 2019).
- OAIC Consumer Complaints Data.

Consumer survey

An external organisation, Roy Morgan Research, was engaged to survey more than 1,000 Australian consumers to share their opinions of consent and gain insight into their perceptions of consent practices followed by various brands. The focus was on how consumers manage their consent when using websites and mobile applications.

Brand analysis

We analysed the branded websites and mobile applications from the top 100 brands in Australia according to a question set developed from the OAIC's consent guidelines. Inputs included the brand's privacy policy and consumer facing website and app features. We also utilised a publicly available cookie scanning tool to test brands' websites for non-essential cookies.

In this index we have not considered other online tracking technologies such as pixels. However, we will look to include these in future editions of the Privacy Index.

References

National

- Privacy Act 1988
- OAIC Consent Guidelines
- ACCC Digital Platforms Inquiry Report – June 2019
- Privacy complaints, FOI reviews on rise in 2018-19
- The OAIC Notifiable Breach Scheme Reports (January-December 2019).

International

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

Top 100 consumer brand

Sources considered in developing the top 100 Australian consumer brands for analysis:

- Privacy Index 2019
- Brand Finance – Top 100 most valuable Australian brands
- AFR and IBISWORLD – top 500 private Australian companies, ranked by company revenue
- Brand Z Australia – top 40 most valuable Australian brands
- Brand Z – top 100 most valuable global brands

Contacts

Partners

David Batch

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

Daniella Kafouris

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

Judith Donovan

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

Tom Rayner

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

David Hobbis

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

Elizabeth Lovett

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

Rachelle Koster

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

About the team

The Privacy experts in our Cyber Risk Practice who developed the Deloitte Australian Privacy Index 2020 included: Marie Chami, Project Manager; Samantha Barr, Project Co-ordinator; Celia Cavanagh, Project Writer; Sebastian Le Cat, Project Writer; Maria Zotti, Project Writer; Vincent Yin, Research; Ansh Sharma, Research.

Deloitte.

MCBD_Syd_06/20_341083206