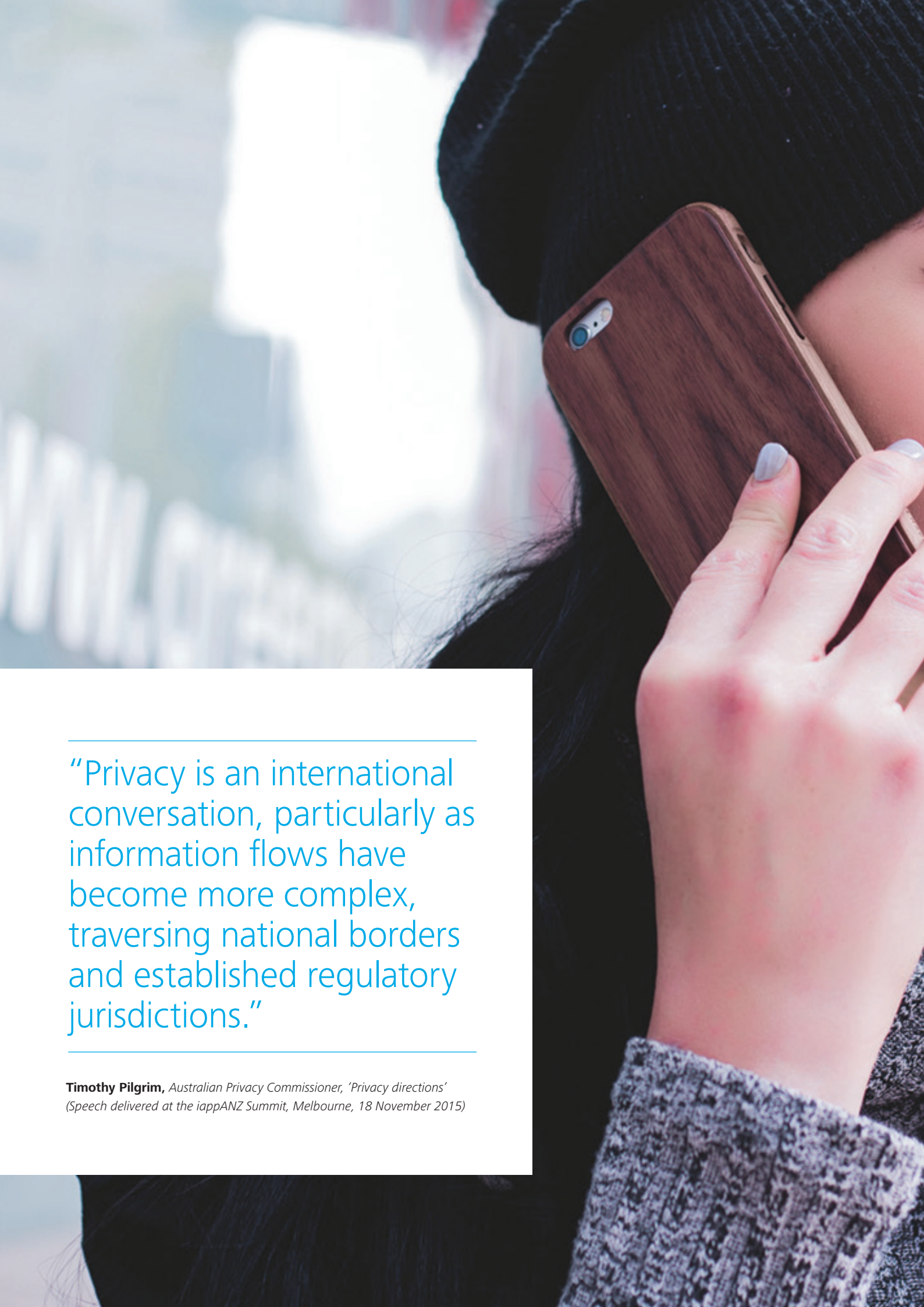
Deloitte.

Deloitte Australian Privacy Index 2016

Trust without borders

Know the worth of risk.



"Privacy is an international conversation, particularly as information flows have become more complex, traversing national borders and established regulatory jurisdictions."

Timothy Pilgrim, *Australian Privacy Commissioner, 'Privacy directions' (Speech delivered at the iappANZ Summit, Melbourne, 18 November 2015)*

Contents

Introduction	4
About this report	5
Executive summary	7
Consumer sentiment analysis	11
Brand analysis	13
Website analysis	15
Mobile application analysis	17
Future trends	19
How would your customers rate you?	23
Methodology	24
References	25
Deloitte Australian Privacy Index 2016	26
Contacts	28

Introduction

In Deloitte's second annual assessment of the privacy practices of more than 100 leading consumer brands operating in the Australian market, a more sophisticated Australian consumer emerges, seeing privacy as a function of both data protection and transparency around how their data is being used.

A more informed consumer has extended the perception of privacy risk from the local market and organisation to the risks associated with sharing information across borders.

In this index Deloitte considers how organisations are positioning themselves for regulatory changes associated with global privacy and data protection. In line with the inaugural index, this year's assessment also includes an analysis of the consumer brands' websites and, for the first time, how the data in their mobile applications are being treated.

Acting globally to foster consumer trust

Consumers are increasingly aware of how their information could be used and are keenly interested in where their information is going. Transparency to build trust has never been more important. Technology trends such as the Internet of Things mean that consumer information can more easily transcend organisational and national borders. It is therefore becoming increasingly important for organisations, to build trust with their customers while protecting, using and sharing their information.

The combination of emerging privacy regulation and the common practice of sharing data have highlighted new types of borders. National borders are the obvious ones, however there are more subtle borders such as those between organisations and their subsidiaries or third parties

Until now, the majority of organisations in Australia have only had to consider local privacy laws. However the need to maximise commercial opportunities, implement efficiencies and reduce costs has led organisations to engage or partner with third party organisations, which are often located overseas and so subject to different and often even more stringent laws. This has meant that Australian-based organisations have to now consider global approaches to managing privacy risks associated with trust and reputation.

Organisations may need to be able to respond to regulator and consumer expectations in the countries in which they operate, as well as mitigating any risks associated with data breaches. The first step is to understand the location of customers and third parties, the countries in which customer data is located, and how the data is used.

Given the impact of continuously changing privacy and data protection requirements around the world, organisations realise that a holistic approach to privacy and data protection is necessary. Many organisations are monitoring, understanding and addressing the challenge of responding to cross-border data risks without necessarily having a presence within a third party organisation or country.

Deloitte Australian Privacy Index 2016

One of the most telling findings in this year's survey is that over 90% of the 1000 participants value trust over convenience – whether that be use of a website or mobile app; a finding that is independent of respondent age.

This indicates to us that organisations have a real opportunity to reposition and grow their ability to proactively build trust with their customers and to safeguard their data no matter where they are.

We hope that the findings in the report and the checklist provided enable your organisation to better self-assess its privacy capability and risks, and begin the dialogue to achieve trust without borders.

We are always happy to discuss any challenges you may be facing and to hear of any comments or feedback you may have; please email:

privacy@deloitte.com.au.

Tommy Viljoen
Lead Partner, Cyber Risk Services, Risk Advisory

Marta Ganko
Privacy and Data Protection Lead, Risk Advisory

About this report

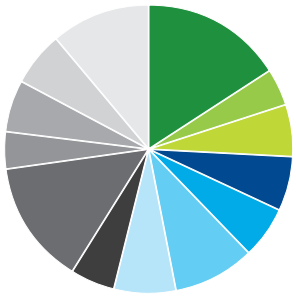
The Deloitte Australian Privacy Index 2016 analyses the state of privacy of 116 of Australia's leading consumer brands in 13 sectors – government, banking and finance, insurance, telecommunications, technology, media, retail, health and fitness, travel and transport, social media, energy, and for the first time, real estate and higher education.

The Index comprises a consumer survey of 1,000 Australian consumers, a website analysis, a mobile app analysis, and a confidential organisational survey.

1000
Australian consumers

116
Consumer brands

13
Sectors



- Banking and finance
- Higher education
- Energy
- Government
- Health and fitness
- Insurance
- Media (news/television/ radio/entertainment)
- Real estate
- Retail
- Social media
- Technology
- Telecommunications (mobile/ internet/home phone)
- Travel andtransport (airlines/agencies/hotels/taxi)

Analysed across four components

1. Consumer sentiment analysis

One thousand Australian consumers were asked to share their opinions of privacy with a particular focus on trust, complaints and information handling expectations. They were asked to consider individual brands and industries.

2. Mobile app analysis

After waking up, 65% of Australians reach for their mobile phone within the first 30 minutes, and 56% of us also connect with our mobiles within the last 30 minutes before sleep[1]. Mobile devices have become the way we connect with the world and for this reason, we analysed the top brands' mobile apps. This included assessing the privacy policies of the apps as well as the way the apps behaved.

[1] http://www2.deloitte.com/au/en/pages/technology-media-and-telecommunications/articles/mobile-consumer-survey-2015.html

Website analysis

The analysis of the privacy policies available publicly on each website was supplemented by how many cookies were placed by the website on the visitor's device, how transparent they were about that and what advice they shared about how to remove them. In addition, this year we included criteria to assess the security practices of various public pages collecting personal information on a website, including the home page, login page and contact forms.

Brand analysis

The internal privacy practices assessed included how policies and procedures were implemented, what training, organisational roles, data breach notification processes, and privacy awareness initiatives were run internally and/or externally. We also included questions on the preparedness of organisations to respond to global regulatory change.

Information was also gathered from surveys and conversations conducted with chief privacy officers, chief risk officers, and employees responsible for legal, risk, data protection and brand.

Nevertheless, we did not include the brand analysis as part of the industry ranking as answers from surveys were opinions and could not be verified. However, these insights are useful when assessing both the perception of and the actual state of privacy of the brands operating in the Australian market.

The caveat is that Deloitte cannot warrant the accuracy of the information gathered nor the extent it may reflect the reality within an organisation. No testing was performed to verify it at any of the organisations. Circumstances might have changed over the period of time this information was gathered.

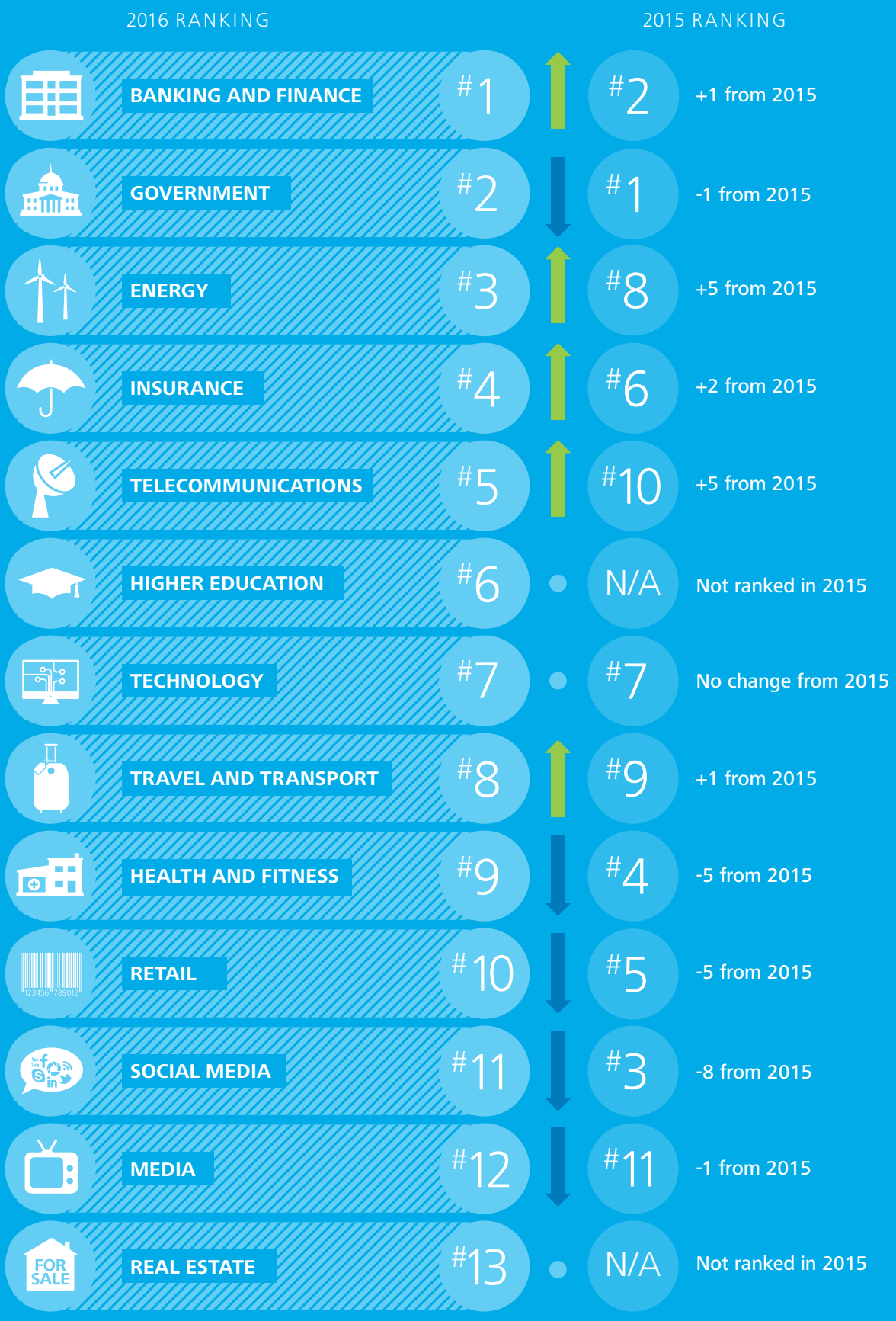
All responses are confidential and only aggregate responses have been reported. Deloitte has compiled the information into a series of graphs. The conclusions drawn about the state of privacy are based on a weighting that was allocated to each of the survey responses and the components considered for the industry ranking.

Thanks and acknowledgement

We would like to thank the following for their support, and for sharing their views and expertise:

- All participating brands in the Deloitte Australian Privacy Index 2016 Survey
- Privacy Sentry Corp for the provision of data via the SpyAware app to complete the mobile app analysis.

Overall ranking



Executive summary

The Index reveals the overall ranking of 13 industry sectors.

The key themes identified were:

94% of consumers believe trust is more important than convenience

Communicating how information is used and shared builds trust

Thinking and acting globally when responding to regulatory change is increasingly necessary.

Overall sector ranking

The following list indicates how industries performed across all areas assessed by the Index according to consumer expectations as well as whether they exhibit good privacy practices. These included:

- Being perceived by consumers as using their information reliably and respectfully
- Implementing adequate security measures when information is submitted via publicly available means
- Informing consumers how their information collected via mobile apps would be used.

Number one in the following list is the most trusted industry with the best perceived governance and the most up-to-date regulatory approach:

1. Banking and finance
2. Government
3. Energy
4. Insurance
5. Telecommunications (mobile/internet/home phone)
6. Higher education
7. Technology
8. Travel and transport (airlines/agencies/hotels/taxi)
9. Health and fitness
10. Retail
11. Social media
12. Media (news/television/radio/entertainment)
13. Real estate

Key insights

- Banking and finance organisations overtook government as leaders in privacy this year as both these heavyweight groups continue to vie for pole position
- When combining the three components assessed, banking and finance organisations took seven positions in the top 10, however the leader in privacy remains a government organisation and government bodies comprise the remainder of the top 10
- Industries in the lower half of the ranking are less regulated in Australia
- Both real estate and higher education – new industries introduced in the 2016 Index – were ranked in the lower half of the industry ranking; although higher education is perceived to be a top five trusted industry by consumers, their websites and mobile apps demonstrate the industry is performing less well than consumers are aware
- The telecommunications industry was the best mover shifting from 10th overall last year to the top five in 2016
- Social media on the other hand plummeted from third position to 11th overall
- Compared with 2015, the number of organisations using a layered approach in their privacy policies has substantially increased.

Characteristics of organisations that did well. They:

- Had mobile apps that communicated to the individual user when they took actions on a mobile device
- Had implemented security protocols on their website when capturing personal information
- Were deemed a trusted brand by consumers
- Have cookies with a shorter expiry timeframe.

Consumer sentiment analysis

The top three most trusted industries as identified by consumers were:

BANKING & FINANCE **GOVERNMENT** **HIGHER EDUCATION**

The three least trusted industries as defined by customers were:

SOCIAL MEDIA **MEDIA** **REAL ESTATE**

Australian consumers are more concerned about sharing the following types of information due to their sensitivity:

71% **CREDIT CARD DETAILS**

65% **I.D. NUMBERS**

34% **MEDICAL RECORDS**

34% **FINGERPRINTS OR FACIAL IMAGE**

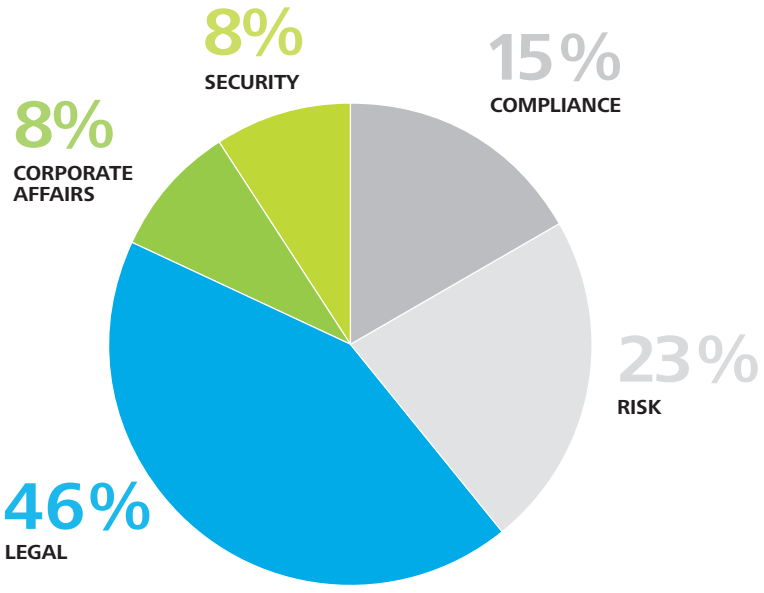
33% **FINANCIAL & CREDIT HISTORY**

After experiencing a privacy issue with an organisation:

94% of consumers consider **trust** more important than the ease of use of a website, app or device.

Brand analysis

Is privacy managed as an operational risk within your organisation?

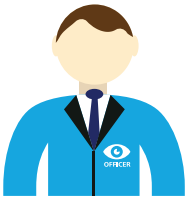


Almost **70%** of organisations conducted a **Privacy Impact Assessment** for business changes.

90% have completed more than five assessments

32% have conducted more than 100 assessments

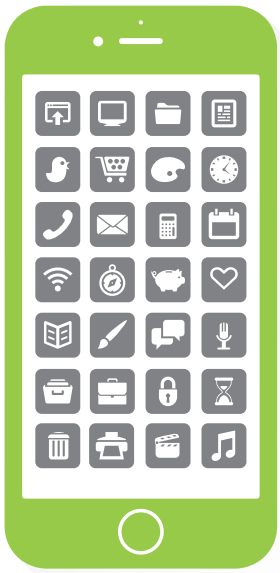
More than **84%** of organisations indicated that there was a **privacy officer role** within the organisation.



73% of the privacy officers manage privacy for the organisation on a full-time basis.

Thought: Is privacy managed as an operational risk within your organisation?

Mobile application analysis



14% of the 88 apps tested accessed user location information

16% of the apps had access permissions to the phone which were not notified prior to installation or on Google Play

The technology sector sent all its data overseas – no data recorded was kept in Australia.

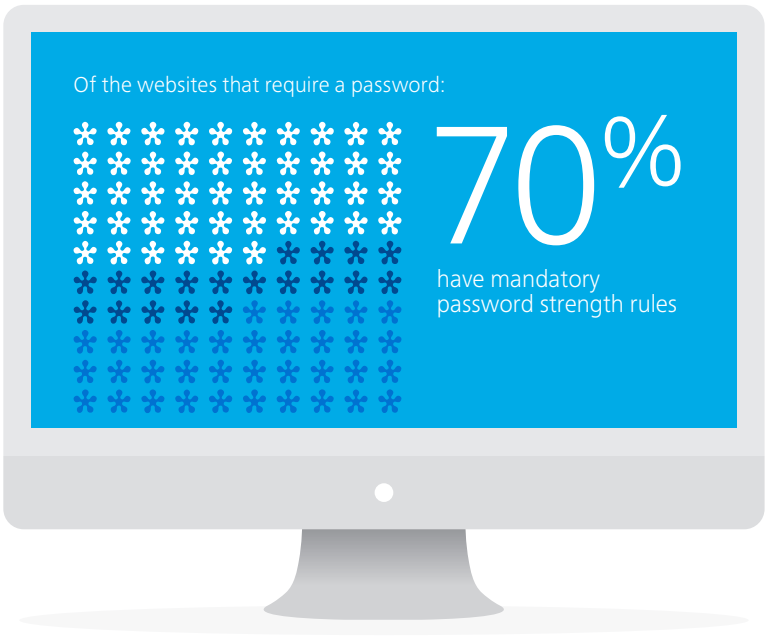
Website analysis

10% of persistent cookies remain stored on a device for **three or more years**

Two-factor authentication is becoming an increasingly popular security option for user authentication, with an overall increase of **15% from 2015 to 2016**

LOGIN

This year almost 30% of brands that included a login option on their website enforced it.



Less than 2% of brands actively notify consumers that cookies are being installed on their devices the first time the home page of their website is visited.

The three **most trusted** industries as identified by consumers:

BANKING & FINANCE

GOVERNMENT

HIGHER EDUCATION

The three **least trusted** industries as defined by customers

SOCIAL MEDIA

MEDIA

REAL ESTATE

Consumers understand and associate the term 'trust' in a range of different ways:

TRUST

60% Reliability

8% Transparency and clear communication

7% Do what you said you would

1% loyalty

1% Don't send personal information to a third party without consent

1% 'needs to be earned'

Around 67% of respondents are concerned with organisations sending personal information outside Australia.

Of this 67%,

40% are **40–64 years old**

10% are **18–25 years old**

29% **would not** like their personal information sent overseas at all

19% **are unsure** whether they would like their personal information sent overseas

13% responded that **nothing would make them more comfortable** when organisations send data overseas

11% would feel **more comfortable if they were asked for permission** before their information was sent overseas

11% would **feel more comfortable** if the reasons for sending their data overseas **were explained beforehand**

Consumer sentiment analysis

Survey participants were asked to indicate up to five brands and industries which they trusted the most and five they trusted the least. Trust was assessed alongside complaints received, as well as how the brands managed their breaches. Participants were also asked specific questions regarding trust.

Industry ranking

The following list indicates which industries consumers trust most with number one being the highest:

1. Banking and finance
2. Government
3. Higher education
4. Energy and utilities
5. Insurance
6. Telecommunications
7. Technology
8. Health and fitness
9. Travel and transport
10. Real estate
11. Retail
12. Media
13. Social media.

Key insights

- Banking and finance and government are the top two most trusted industries when it comes to safeguarding personal information
- Consumers aged between 18 and 25 are more concerned about sharing mobile numbers or browsing history than medical records
- Consumers aged between 26 and 39 are more concerned about sharing their address than their medical records
- 71% of the 1000+ consumers surveyed had never had a privacy issue with a brand. The remaining 29% cited 851 privacy issues with organisations included in the survey
- The industry with the highest average number of privacy issues was social media, followed by government
- Travel and transport had the lowest privacvy issues.

Looking at three main areas

Trust

- 30% of the public picked the same government organisation as their most trusted
- Five of the top ten most trusted organisations were from the government sector with the other five from banking and finance
- The five least trusted organisations were in the social media sector
- The top five most trusted organisations that consumers currently use or have used in the past were in banking and finance or government
- The five least trusted organisations that consumers had either stopped using or have never used due to negative privacy perceptions were in social media.

Complaints

- The industries with the highest average number of complaints were social media and telecommunications. Travel and transport had the lowest number of complaints
- More than 9% of total complaints were related to the same telecommunication organisation
- We complain more about privacy as we get older. Less than 8% of 18-25 year olds have made a privacy complaint, while more than 38% of 40-64 year olds have made a privacy complaint. These are similar results to the 2015 Privacy Index
- The most common type of complaint was information being used inappropriately (17%), followed by organisations failing to secure personal information (16%)
- 52% of consumers were satisfied with how their complaint was resolved.

Notification

- 14% of respondents had received a privacy notification following a data breach. Of those that had been notified of a breach:
  - 33% trusted that organisation more compared with 29% who reported trusting the organisation less (4% difference). In 2015 there was a 7% differential with 34% trusting the brand more and 27% trusting it less after a breach notification.
  - **A significant 71% did not trust the organisation any less following the notification, slightly down from 73% in 2015.**

Sending data overseas

- Around 67% of respondents are concerned with organisations sending personal information outside Australia.

Consumer preferences

- More than 21% want detailed information if organisations send their information to third parties, including to whom and why
- 14% want to know how their personal information is protected
- More than 7% want to know if their information is being sold to other companies.

Organisations that did well

- Are perceived by consumers as most trusted
- Are in regulated industries
- Had the least privacy issues and complaints
- Notified their customers of any data breaches that occurred, which led the customers to trust the organisation more.

46% OF ORGANISATIONS

Given the new European Union Data Protection regulations introduced in April 2016 and effective in 2018, 46% of the organisations surveyed indicated that they had European citizen customers.

MORE THAN 15% OF ORGANISATIONS

More than 15% were not sure whether they did have European citizens as customers. Of the almost half of the organisations surveyed that indicated they had European citizen customers, more than 80% have considered how global changes such as the EU General Data Protection Regulation will impact their organisation.

METHODS OF PROTECTING PERSONAL INFORMATION

- Anonymisation or de-identification processes
- Policies and procedures
- Right to audit clauses in contracts
- Mandatory privacy training
- External threat monitoring for example, vulnerabilities or hackers
- Encrypt information stored
- Encrypt information sent
- Mobile device management –
- Issue corporate mobile devices to staff
- Identity and access management solution
- Data Leakage Protection –
- Data minimisation
- Consent/secondary purpose management
- Double/triple blindness

Brand analysis

Privacy capabilities within organisations are maturing. Deloitte analysis was performed on leading consumer brands to measure the maturity of privacy management within their organisation, security measures to protect data which have been implemented, and preparedness for global regulatory change.

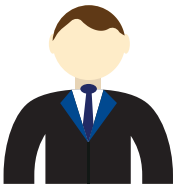
Key insights

Almost 70% of organisations have either developed or determined to develop a privacy strategy. Two-thirds of these organisations have refreshed their strategy in the last 24 months. One third did so for compliance reasons, while the remainder did so to build trust with their customers or employees.

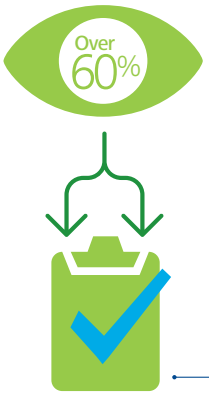
- All organisations considered building trust with their customers as a competitive advantage
- More than 84% of organisations indicated that there was a privacy officer role within the organisation
- 73% of them manage privacy for the organisation on a full-time basis
- All organisations had a customer-facing privacy policy available online
- More than 60% have it also available in hard-copy format
- Most organisations (92%) also have an internal privacy policy that defines 'personal information' and identifies how it should be managed
- Almost a third of organisations had considered receiving consent from consumers in an alternative way to 'ticking a box'
- More than two-thirds of organisations participate in Privacy Awareness Week
- All organisations have internal privacy training, 85% of which make these compulsory
- More than two-thirds of organisations had published privacy awareness or education materials in the last 12 months, mostly internal training materials
- More than two thirds of the organisations surveyed had a data breach policy
- 80% of them conduct training for their employees in their data breach notification policy and procedures.

More than 90% of organisations internally logged and reported all privacy incidents and data breaches.

Almost 90% of the assessed organisations that had a data breach within the last 24 months impacting more than 50 records notified the CEO of the breaches.



Almost
90%



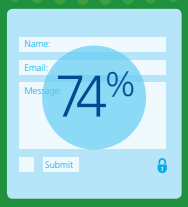
More than 60% of organisations surveyed had a process in place to review whether third parties are compliant with their privacy requirements. Almost all of them carry out this process during the contract review stage. Others have an annual review process or only perform a due diligence process at the start of the contract.

The brand assessment was not considered for the industry ranking as Deloitte was unable to verify the answers provided. However, useful insights were provided as to the state of privacy of brands operating in the Australian market. Not all organisations invited to participate in the survey responded to the survey.

OF THE WEBSITES THAT REQUIRE A PASSWORD

70%

HAVE MANDATORY PASSWORD STRENGTH RULES
However the remaining 30% did not require a complex password accepting the password "123"



74% OF THE BRANDS THAT INCLUDED A CONTACT FORM
on their website provided SSL/TLS protection for data transmitted through those forms

LESS THAN 2%

LESS THAN 2% OF BRANDS ACTIVELY NOTIFY CONSUMERS
that cookies are being installed on their devices the first time they visit the website

COOKIES

10% of persistent cookies remain stored on a device for **three or more years**

The health and fitness sector recorded the lowest average number of third party cookies per site, averaging only **one third party cookie.**

The media sector recorded the highest number of third party cookies, averaging **12 third party cookies** per site.

Website analysis

The website analysis of the brands involved assessing online privacy policy, security measures applied on key pages of the website, and the cookies the website stores on the devices of visitors.

This year for the first time, Deloitte assessed the type of security protocol implemented on a website. The security protocols that were assessed include Secure Socket Layer (SSL) or and Transport Layer Security (TLS).

Government and banking and finance again performed the best in the website component of the Index:

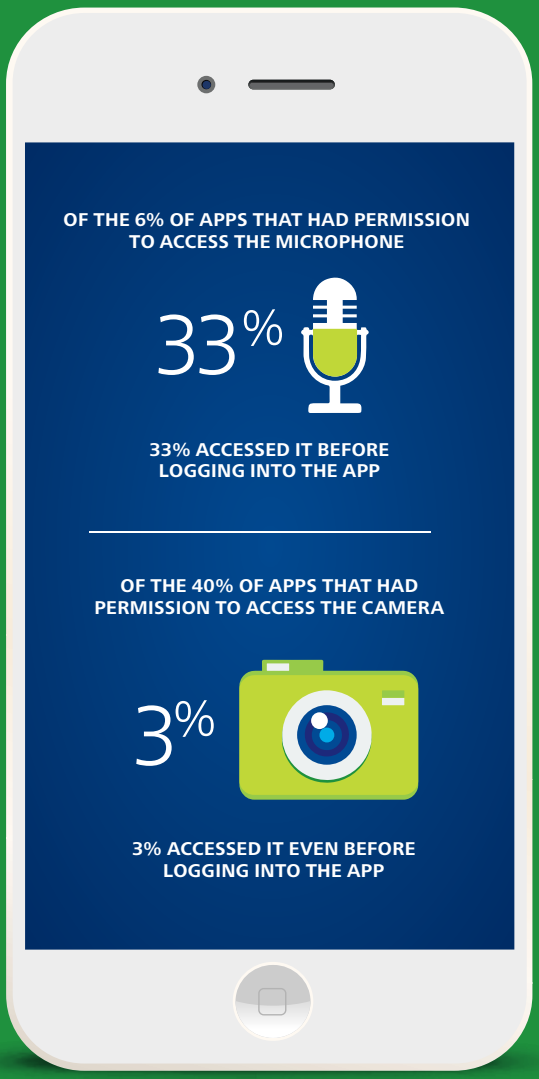
1. Government
2. Banking and finance
3. Social media
4. Energy
5. Health and fitness
6. Insurance
7. Retail
8. Telecommunications
9. Higher education
10. Travel and transport
11. Real estate
12. Technology
13. Media.

Key insights

- There was a 58% increase in 'layered privacy policies' by brands this year compared with 2015
- Two-factor authentication is becoming an increasingly popular option for verifying user details, with an overall increase of 15% from 2015 to 2016. This year almost 30% of brands that included a login option in their website enforced it
- This phenomenon is particularly evident in the banking and finance industry where 74% brands have implemented two-factor authentication, followed by government and technology, with each at 43%
- The technology industry had the most up-to-date privacy policies with 71% of brands providing privacy policies that were updated/published within the last 12 months
- Of the privacy policies assessed, 18% were last updated/published prior to the Australian Privacy Principles effective date 12 March 2014, and only 12% within the last six months. The oldest policy had not been reviewed for three years
- 38% of brands tested provide a SSL/TLS secured home page, with the social media industry performing the best, having 100% of the brands tested using a secure protocol
- 91% of brands with a login page provide an SSL/TLS secured login page
- Of this, almost 90% supported the latest version of TLS across their website
- Almost a quarter of brands provide a detailed list of countries to which data are disclosed. The energy industry performed best, with 100% providing a detailed list
- 33% of the brands provide supporting materials to help the reader understand key messages from their privacy policy
- There was a 16% decrease in the average time a cookie is stored on a device across all brands since last year
- The average time a cookie is stored on a device is 657 days or 1.8 years
- More than half of the persistent cookies remain stored on a device for more than a year
- The media sector recorded the highest average number of cookies remaining on a device after closing a web browser for a second year in a row, with an average of 24 persistent cookies remaining per site.

Organisations that did well:

- Had updated their privacy policies within the last six months
- Had a layered privacy policy
- Provided a complete list of countries to which information is disclosed
- Had session cookies rather than persistent cookies
- Had defined password rules where a login was required
- Had few third party cookies
- Provided and enforced SSL/TLS encryption when viewing and interacting with their web page.



When data was sent to the following locations:
Australia, United States, Germany, Japan, Hong Kong, Singapore and Ireland

only 5% of the apps analysed kept all of their data in Australia.

Mobile application analysis

Mobile applications of the brands were assessed to determine whether the application reflected what a consumer was notified of from their policies. Application behaviour was assessed without logging into the app. Not all brands had a mobile application available for assessment.

Industry ranking

The list below indicates how industries performed against the defined mobile analysis metrics of the Index, with number one ranked the best:

1. Telecommunications
2. Banking and finance
3. Government
4. Media
5. Retail
6. Social media
7. Technology
8. Travel and transport
9. Energy
10. Insurance
11. Real estate
12. Health and fitness
13. Higher education.

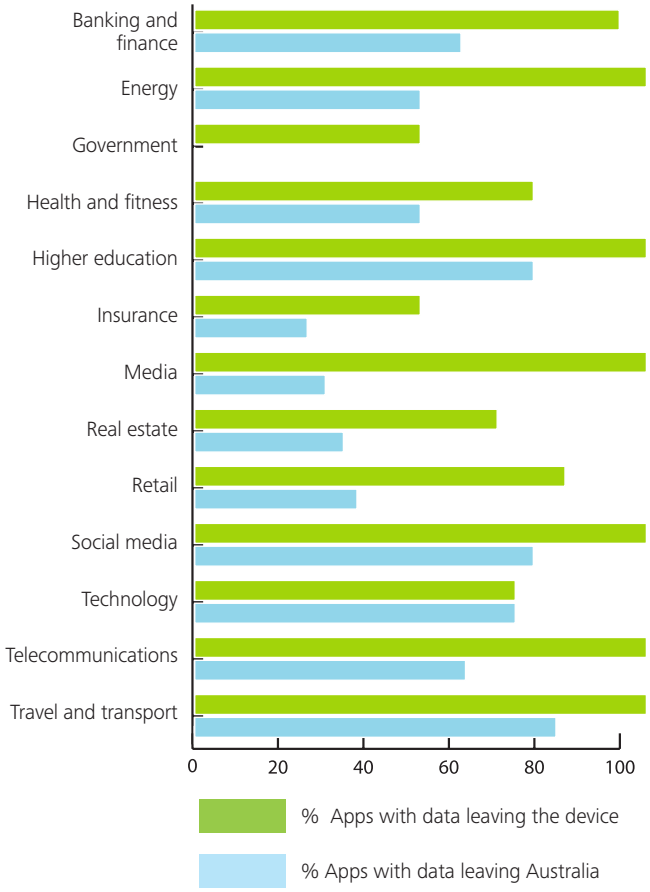
Key insights

Access to location

- 14% of the 88 apps tested accessed user location information
- The telecommunications industry's apps accounted for the majority of location access events (90%), followed by social media mobile apps (6%) and travel and transport mobile apps (3%)
- Apps from banking and finance, energy, government, higher education and insurance do not access location information from a mobile device.

Information leaving a mobile device

- 85% of the apps analysed made a connection to send or receive data from a location (including Australia)
- The technology sector sent and received the most data (35%), followed by travel and transport (30%) and retail (7%)
- Overall, the government, energy, and insurance sectors sent and received the least data
- 81% of the apps sent data overseas. Of this, 97% of the apps transferred data to the United States, 14% went to Singapore, 4% went to Hong Kong, 4% to Germany, 6% to Ireland and 1% to Japan.



Privacy policies

- 99% of brands implemented layered privacy policies in their apps
- 28% of apps did not have an accessible privacy policy before login. Of these, 45% did not have a privacy policy accessible from Google Play. Yet 96% of the apps transferred user information in or out of the device without logging in
- 52% of brands provided a detailed list of countries to which they disclose privacy data. The banking and finance industry performed best with 76% of app brands tested providing a detailed list. This was closely followed by government and real estate.

Organisations that did well:

- Had mobile apps with a policy notification
- Provided a complete list of countries to which they disclose data
- Allowed users to restrict application permissions.

‘Tensions between different legal systems such as the European Union and the United States result in loss of confidence on the part of users and confusion by commercial entities.’

2015 International Conference of Privacy and Data Protection Commissioners
(Full report presented in Amsterdam, 28 October 2015)

Future trends

The Mandatory Data Breach Notification bill and text of the EU General Data Protection Regulation released in April 2016 have caused organisations with European operations to review and begin proactively managing their personal information use and the third parties with custody of their customers' information.

Privacy and data protection continue to generate discussion and be boardroom agenda items, as consumers want to know how their information is used and with whom it is being shared.

These encouraging actions by organisations indicate that the risk of reputational loss and consumer trust, and its impact on the bottom line, is well understood.

What are the key trends your organisation needs to be made aware of?

Trend 1: Consumers are becoming more discerning

- Consider whether consumers should be part of your privacy strategy
- As consumers are becoming increasingly aware of how organisations are using and handling their personal information you need to consult more about your use of their data
- You should alert consumers to any risks they face when sharing their personal information

- Consider what you need to do as consumers become more cautious about what information they choose to exchange in return for an organisation's products and services
- As consumers seek transparency from the organisations and brands with which they transact you should find ways to meet this need.

The above statements reflect the way that consumers understood and associated the word 'trust' in our consumer survey.

An increased understanding of privacy can change the way that consumers interact with organisations, and the way they purchase goods and services.

If consumer privacy expectations are not met, organisations risk:

- losing the trust of consumers
- tainting their brand and reputation
- receiving inaccurate or fabricated personal information which becomes part of the organisational decision-making processes, and which potentially costs more money to remediate.

By enhancing products and services to suit consumer expectations, and treating privacy as a complementary service or product feature, rather than a compliance issue, an organisation can build a better relationship with the consumer and make sure that their customers become a key part of building their brand.

Trend 2: Consumers want choice

- Should organisations have an ethical obligation to manage consumers' personal information in line with best practice and expectations?

94% of consumers consider 'trust' more important than the 'ease of use of a website', app or device.

More opportunities for using information other than for primary business purposes have forced organisations to obtain consent from individuals for these additional uses. This tends to be in the form of bundled consent. A move towards dynamic opt-in consent allows users and consumers to select any additional uses for their information at the time of transaction. This is reflected in the concern 67% of respondents have with organisations sending their personal information outside Australia. More than 21% of respondents like to be informed if organisations send information to third parties.

It is important that organisations pay attention to consumer expectations to ensure they are:

- Informing consumers exactly how their information will be used
- Giving consumers the power to decide what they want their information used for.

Poor consent management can result in:

- Legal action and/or regulator penalties and sanctions
- Reputational damage
- Handling of personal information misaligned with consumer expectations
- Backlash from consumers
- Reduced demand for the organisation's products and services.

Good consent management practices can:

Increase consumer loyalty and trust

Ensure the organisation personalises their consumers' experience by meeting consumer expectations transparently

Leverage big data insights with confidence.

Trend 3: Increased and active management of third parties

Organisations are focusing more on their core business functions and are outsourcing peripheral functions to increase operational efficiency.

Third party management is becoming increasingly complicated due to third party contractors sub-contracting parts of their services to 'fourth parties' etc.

Organisations are responsible to protect the personal information they have collected. This includes information passed on to third parties.

Poor third party selection and management may result in:

- Information being mishandled
- A lack of communication between third parties and the organisation
- Penalties being imposed on an organisation by regulators
- Legal action taken against an organisation by consumers in the form of a civil suit
- Reputational damage
- Loss of consumers.

Transparent third party management practices enable:

Communication and cohesive operations between an organisation and its third parties with respect to handling personal information

Trust and a positive reputation among consumers

Control and oversight of how data are used and protected

Minimised legal liability and risk associated with third parties misusing this data.

The survey of brands indicates that more than 60% of organisations have active governance procedures and review privacy requirements of third parties during contract renewal time. It will become more important to operationalise the reviews of these third parties and ensure they become part of an organisation's first line of defence.

Trend 4: Global approaches to privacy and data protection management

Organisations are beginning to take a global approach to managing privacy and data protection risk exposure. The risk exposure is largely driven by regulatory change such as the EU General Data Protection Regulation and stricter requirements regarding cross border data transfers.

As organisations expand their operations, customer bases become global and third parties are engaged to support business functions. Thinking and acting globally become critical success factors.

Customer expectations also need to be managed.

>21% would like to be informed if organisations send their information to third parties

7% indicated that they would like to know if their information is being sold to other companies.

If organisations do not take a global approach to privacy they risk lagging behind. The implications include:

- Misaligned consumer expectations affecting the ability of a brand to operate in certain jurisdictions
- Loss of global and local market share of customers
- lower resilience to regulatory change
- Exposure to penalties and sanctions imposed on an organisation if regulations are violated.

By addressing privacy risk with a global lens organisations will be better able to:

Significantly minimise business disruption

Share data across borders with confidence

Develop regulatory compliance resilience earlier

Build trust between the organisation's locations, third parties, regulators and consumers.

Trend 5: Balancing data commercialisation and consumer choice

Many consumers believe that organisations use their information to drive further revenue. Apart from some social media and technology organisations which indicate this explicitly, customers know little about what organisations are actually doing with their information and they want to know. The risk is that when this information is revealed, consumer anger and publicity could seriously damage the brand.

The opportunity for organisations to manage this risk is to build trust with customers by informing them of their commercial use of customer information, and offer a choice as to what the consumer would like their personal information to be used for. This will ensure that organisations can confidently and ethically earn any additional revenue with their customers' consent.

'The constant flow of information is the lifeblood of our daily interactions. The distribution of data across different platforms and borders is shifting traditional social, economic and geo-political boundaries, and creating a more integrated and interconnected global ecosystem.'

Thomson Reuters, 'Face to Face with Stephen Wong, Privacy Commissioner for Personal Data' *(Hong Kong, January 2016)*

‘A leadership commitment to a culture of privacy is a foundation for good privacy governance. Good privacy governance can improve business productivity and help to develop more efficient business processes.’

Office of the Australian Information Commissioner (OAIC), ‘Privacy Management Framework: Enabling Compliance and Encouraging Good Practice’ *(Sydney, 2016)*

How would your customers rate you?

MOST TRUSTED

Our customers are better off after we use their information

TRUSTED MORE

We give our customers a choice as to how their information is used/shared. Where we don't, we explain why

TRUSTED A LITTLE

We listen to our customers' concerns and attempt to incorporate their feedback. We give our customers some choice as to how their information is used or shared. Some of our customers are better off

TRUSTED A LITTLE

We tell our customers what we do with their data, but we don't give them a choice as to how it is used or with whom it is shared

LEAST TRUSTED

We are compliant, but we know we hide the real story regarding customer usage in our privacy policy

LEAST TRUSTED

We sometimes try to comply with the Australian privacy requirements

LEAST TRUSTED

Our organisation is not required to comply with privacy requirements so we don't

Methodology

The Deloitte Australian Privacy Index 2016 is the result of analysing 116 of Australia's leading consumer brands. It is an annual report that measures the state of privacy across 13 sectors.

The input for the Deloitte Australian Privacy Index 2016 report comprised:

1. Survey of 1000 Australian consumers' sentiment
2. Website analysis
3. Mobile application analysis
4. Confidential organisational survey.

Consumer sentiment analysis

An external organisation was engaged to survey 1000 Australian consumers to share their opinions of privacy with a particular focus on trust and complaints. Some questions focused on specific industries or brands.

Website analysis

The website analysis of the brands involved assessing:

- The online privacy policy
- Cookies placed on a device

The final score for this section was calculated on these two inputs. The online privacy policy analysis was weighted 60% and the website technology analysis 40%.

Online privacy policy analysis

The online privacy policy was assessed based on a range of criteria including the privacy policy, compliance, adoption of guidelines set out by the Office of the Australian Information Commissioner, and availability of supporting materials including videos to assist consumers understand the privacy policy of the brand.

Website technology analysis

The website technology analysis comprised:

- Cookies placed by the website on the visitor's device
- Solutions implemented to protect communications between the visitor and the website of the brand.

Cookies

A custom built tool was used to capture the cookies that were placed on the visitor's device.

Each website was assessed for the number of first and third party cookies placed on the visitor's device. The cookie type was identified as either session or persistent, and the expiry time of the cookie was also considered.

Each brand was also assessed on the level of encryption when transferring data over the internet. Specific emphasis was placed on the type of encryption used, i.e. whether Secure Socket Layer (SSL) or Transport Layer Security (TLS) or both.

Mobile application analysis

The mobile application analysis of the brands involved assessing:

- App behaviour
- Recipient countries for data leaving the app
- App privacy policy.

Mobile app technology implementation analysis

To conduct the analysis, a third party app, SpyAware was downloaded onto the device. Designed to reveal the hidden activities of apps, SpyAware examines every eight seconds which apps are active and which sensors or radios are in use. This enabled mobile apps to be assessed based on the app's logged behaviour, compared with the permissions requested on app installation, and the permissions present on the Google Play store creating a privacy profile for each app.

For each brand, the most recent version of their most popular app was selected for assessment. Although Apple is currently winning the local device competition, Android remains the dominant operating system, with Australian sales surpassing iOS almost every month over the past year.[2] For this reason, only apps available for Android devices were considered. The apps were tested on a Galaxy Core Prime Lollipop on Android version 5.1.1. Android Lollipop users account for majority of the Android OS market (36%)

Mobile app privacy policy analysis

The privacy policies on the mobile apps were assessed according to the same criteria as the website policies.

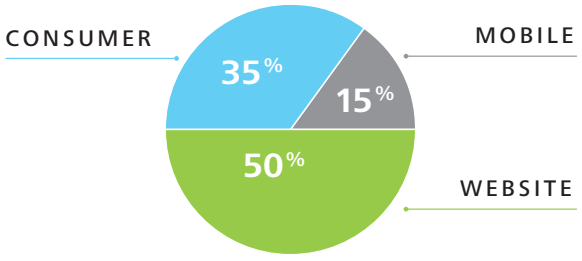
88 out of 116 brands had a mobile app. Where a brand did not have an app, the consumer survey and website analysis comprised 100% of the score.

Organisational survey

Brand analysis was not a component considered for the industry ranking, as answers received from surveys could not be independently verified.

Overall index result

The overall score and Index ranking comprised the website analysis, consumer sentiment analysis and mobile app analysis.



2 Deloitte Australia http://www2.deloitte.com/au/en/pages/technology-media-and-telecommunications/articles/mobile-consumer-survey-2015.html

References

Regulations

National laws

Privacy Act 1988 (Cth)

Other national laws

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)
Crimes Act 1914 (Cth)
Data-matching Program (Assistance and Tax) Act 1990 (Cth)
Freedom of Information Act 1982 (Cth)
National Health Act 1953
National Health Act 1953 (Cth)
Personally Controlled Electronic Health Records Act 2012 (Cth)
Personal Property Securities Act 2009 (Cth)
Spam Act 2003 (Cth)

State laws

Freedom of Information Act 1992 (WA)
Health Records Act 2001 (ACT)
Health Records and Information Privacy Act 2002 (ACT)
Health Records (Privacy and Access) Act 1997 (ACT)
Information Act (NT)
Information Privacy Act 2014 (ACT)
Information Privacy Act 2009 (QLD)
Personal Information and Protection Act 2004 (TAS)
Privacy and Data Protection Act 2014 (ACT)
Privacy and Personal Information Protection Act 1998 (ACT)

There are also privacy codes as well as industry standards that contain privacy requirements.

Other references

2015 International Conference of Privacy and Data Protection Commissioners (Full report presented in Amsterdam, 28 October 2015): https://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf

Deloitte Australia: http://www2.deloitte.com/au/en/pages/technology-media-and-telecommunications/articles/mobile-consumer-survey-2015.html

Office of the Australian Information Commissioner (OAIC), 'Privacy Management Framework: Enabling Compliance and Encouraging Good Practice' (Sydney, 2016): https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework

Privacy Sentry Corp: http://privacysentrycorp.com/

SpyAware: http://spyaware.be

Thomson Reuters, 'Face to Face with Stephen Wong, Privacy Commissioner for Personal Data' (Hong Kong, January 2016): http://www.hk-lawyer.org/content/face-face-stephen-wong-privacy-commissioner-personal-data

Timothy Pilgrim, Australian Privacy Commissioner, 'Privacy directions' (Speech delivered at the iappANZ Summit, Melbourne, 18 November 2015)

"Any organisation which shares data has become a data broker of some sort. So what does that mean? As organisations collect and share more of their customers' data with external parties, consumer confidence, trust, choice, as well as commercial interests become important elements to balance in an increasingly digitally borderless world. This requires organisations to break down their own borders and operate transparently to continue building trust with consumers."

Marta Ganko, Cyber Risk Services, Deloitte Australia

Deloitte Australian Privacy Index 2016

2016 Deloitte Australian Privacy Index – Overall organisation ranking per industry

Rank	Brand industry
1	Government
2	Banking and finance
3	Banking and finance
4	Banking and finance
5	Banking and finance
6	Banking and finance
7	Government
8	Banking and finance
9	Government
10	Banking and finance
11	Banking and finance
12	Government
13	Banking and finance
14	Banking and finance
15	Banking and finance
16	Government
17	Technology
18	Banking and finance
19	Energy
20	Banking and finance
21	Banking and finance
22	Banking and finance
23	Insurance
24	Telecommunications (mobile/internet/home phone)
25	Government
26	Insurance
27	Insurance
28	Higher education
29	Retail

Rank	Brand industry
30	Banking and finance
31	Energy
32	Technology
33	Technology
34	Telecommunications (mobile/internet/home phone)
35	Energy
36	Banking and finance
37	Telecommunications (mobile/internet/home phone)
38	Energy
39	Energy
40	Insurance
41	Energy
42	Insurance
43	Insurance
44	Retail
45	Travel and transport (airlines/agencies/hotels/taxi)
46	Travel and transport (airlines/agencies/hotels/taxi)
47	Social media
48	Telecommunications (mobile/internet/home phone)
49	Health and fitness
50	Telecommunications (mobile/internet/home phone)
51	Travel and transport (airlines/agencies/hotels/taxi)
52	Banking and finance
53	Banking and finance
54	Travel and transport (airlines/agencies/hotels/taxi)
55	Higher education
56	Higher education
57	Retail
58	Retail

Rank	Brand industry
59	Energy
60	Health and fitness
61	Health and fitness
62	Retail
63	Retail
64	Insurance
65	Insurance
66	Technology
67	Travel and transport (airlines/agencies/hotels/taxi)
68	Retail
69	Higher education
70	Travel and transport (airlines/agencies/hotels/taxi)
71	Travel and transport (airlines/agencies/hotels/taxi)
72	Government
73	Media (news/television/radio/entertainment)
74	Higher education
75	Travel and transport (airlines/agencies/hotels/taxi)
76	Social media
77	Retail
78	Real estate
79	Media (news/television/radio/entertainment)
80	Retail
81	Telecommunications (mobile/internet/home phone)
82	Insurance
83	Retail
84	Health and fitness
85	Media (news/television/radio/entertainment)
86	Technology
87	Health and fitness

Rank	Brand industry
88	Travel and transport (airlines/agencies/hotels/taxi)
89	Media (news/television/radio/entertainment)
90	Retail
91	Health and fitness
92	Travel and transport (airlines/agencies/hotels/taxi)
93	Travel and transport (airlines/agencies/hotels/taxi)
94	Health and fitness
95	Social media
96	Retail
97	Telecommunications (mobile/internet/home phone)
98	Technology
99	Technology
100	Travel and transport (airlines/agencies/hotels/taxi)
101	Real estate
102	Real estate
103	Travel and transport (airlines/agencies/hotels/taxi)
104	Insurance
105	Social media
106	Media (news/television/radio/entertainment)
107	Retail
108	Media(news/television/radio/entertainment)
109	Social media
110	Retail
111	Retail
112	Media (news/television/radio/entertainment)
113	Real estate
114	Real estate
115	Media (news/television/radio/entertainment)
116	Retail

Contacts

Sydney
Tommy Viljoen
Partner, Risk Advisory
+61 2 9322 7713
tfviljoen@deloitte.com.au

Melbourne
Greg Janky
Partner, Risk Advisory
+61 3 9671 7758
gjanky@deloitte.com.au

Melbourne
Puneet Kukreja
Partner, Risk Advisory
+61 3 9671 8328
pkukreja@deloitte.com.au

Sydney
Marta Ganko
Risk Advisory
+61 2 9322 3143
mganko@deloitte.com.au

www2.deloitte.com/au/privacy-index

MCBD_MEL_04/16_052710