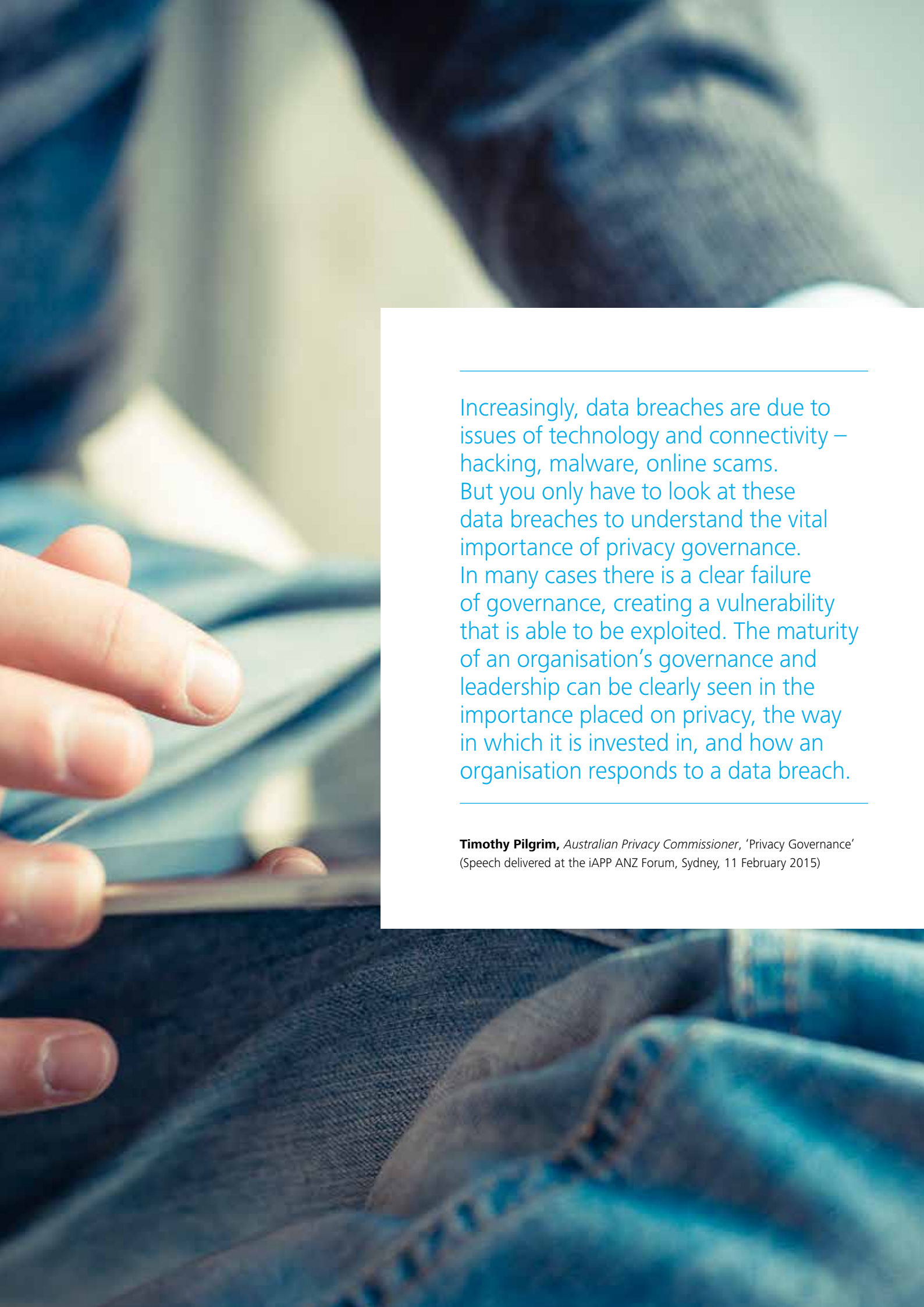
Deloitte.

Deloitte Australian Privacy Index 2015

Transparency is opportunity

Know the worth of risk.



Increasingly, data breaches are due to issues of technology and connectivity – hacking, malware, online scams. But you only have to look at these data breaches to understand the vital importance of privacy governance. In many cases there is a clear failure of governance, creating a vulnerability that is able to be exploited. The maturity of an organisation's governance and leadership can be clearly seen in the importance placed on privacy, the way in which it is invested in, and how an organisation responds to a data breach.

Timothy Pilgrim, *Australian Privacy Commissioner*, 'Privacy Governance' (Speech delivered at the iAPP ANZ Forum, Sydney, 11 February 2015)

Contents

Introduction

In an Australian first, Deloitte has assessed leading consumer brands operating in Australia on the perception of their privacy risk.

Deloitte assessed 100+ leading consumer brands against privacy best practices. This included an analysis of their websites, the attention each of these brands received in the media around their protection of data, and a survey of more than 1000 consumers as to their perspective of privacy across 11 industry sectors.

Emerging privacy risks

There is increased sensitivity among individuals and organisations regarding the use and disclosure of information. Consumer awareness of emerging privacy risks is growing given both increased media attention and regulatory change occurring around the world. This means that privacy is more than a legal and compliance issue. Knowing the damage a privacy breach can do to the reputation of an organisation, via traditional and social media channels, needs to be better understood and managed.

In addition privacy issues no longer just have a local impact but can and do extend globally, driven by the power to amplify across digital channels, organisational global expansion and the use of 'cloud' technologies.

To date organisations have tended to focus on compliance and protecting customer information with various security measures. However, the management of the collection, use, disclosure of information has been left behind. As the Gartner report published in 2014 states, privacy today is where security was ten years ago.[1]

As an evolving discipline, every organisation needs to understand how to measure the risks inherent in privacy protection and breach, and how best to receive a return on this investment. To get a clear handle on this the first step is to be clear how your organisation in all its complexity understands how its information is collected, used and disclosed.

In many of the organisations with which we work, managing privacy risk is key considering the challenges in a constantly evolving technology and regulatory landscape.

Deloitte Australian Privacy Index 2015

Given the importance of consumer trust and reputational risk management – a number one strategic risk for organisations globally – we are presenting this inaugural index as an empirical way to measure and highlight the areas where we are doing well and where we need to continue to get better at improving our trust rankings over the coming years.

We hope the findings and insights in this report will be a useful way to open the conversation on privacy and how best to manage these risks.

We look forward to catching up with many of you to discuss the findings in more detail but in the meantime please reach out to: *privacy@deloitte.com.au* with any comments or feedback.

Tommy Viljoen
Partner, Risk Services

Gavin Cartwright
Cyber Risk Services

[1]Gartner, *Hype Cycle for Privacy*, 18 July 2014.

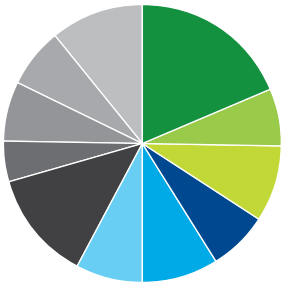
About this report

The Deloitte Australian Privacy Index 2015 is the result of analysing 104 of Australia's leading consumer brands. It is an annual report that measures the state of privacy across 11 sectors. The sectors covered are Government, Banking & Finance, Insurance, Telecommunications, Technology, Media, Retail, Health & Fitness, Travel & Transport, Social Media, and Energy. The input for the Deloitte Australian Privacy Index 2015 report comprises of a consumer survey of 1000 Australian consumers, a website analysis, a media review, and a confidential organisational survey.

1000
Australian consumers

104
consumer brands

11
sectors



- Banking & Finance
- Energy
- Government
- Health & Fitness
- Insurance
- Media (news, television, radio, entertainment)
- Retail
- Social Media
- Technology
- Telecommunications (mobile, internet, home phone)
- Travel & Transport (airlines, agencies, hotels, taxi)

Analysed across 4 components

Consumer sentiment analysis

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

Brand analysis

The internal privacy practices assessed included how policies and procedures were implemented, training, organisational roles, data breach notification processes, and how privacy awareness initiatives were run internally and/or externally. Information was gathered from surveys and conversations conducted with Chief Privacy Officers, Chief Risk Officers, and employees responsible for legal, risk, data protection and brand.

Brand analysis was not a component considered for the industry ranking as answers received from surveys could not be verified. However, useful insights were provided as to the state of privacy of brands operating in the Australian market.

Media sentiment analysis

Media sentiment of privacy was assessed across mainstream online media[2] and user generated content[3].

Mainstream online media considered for assessment started for the 12 months commencing 1 April 2014. The user generated content considered for assessment started 90 days before the 1 April 2015. With user generated content over 25000 followers or more only considered sufficiently influential for scoring purposes.

Website analysis

Deloitte conducted an internal analysis of the privacy policies available publicly on each website as well as the cookies placed by the website on the visitor's device.

Deloitte makes no representation or warranty about the accuracy of the information or how closely the information gathered in the surveys resembles the reality within an organisation. No testing was performed at any of the organisations. Circumstances might have changed over the period of time this information was gathered, and this report is not able to take any such changes into account in this inaugural edition.

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.

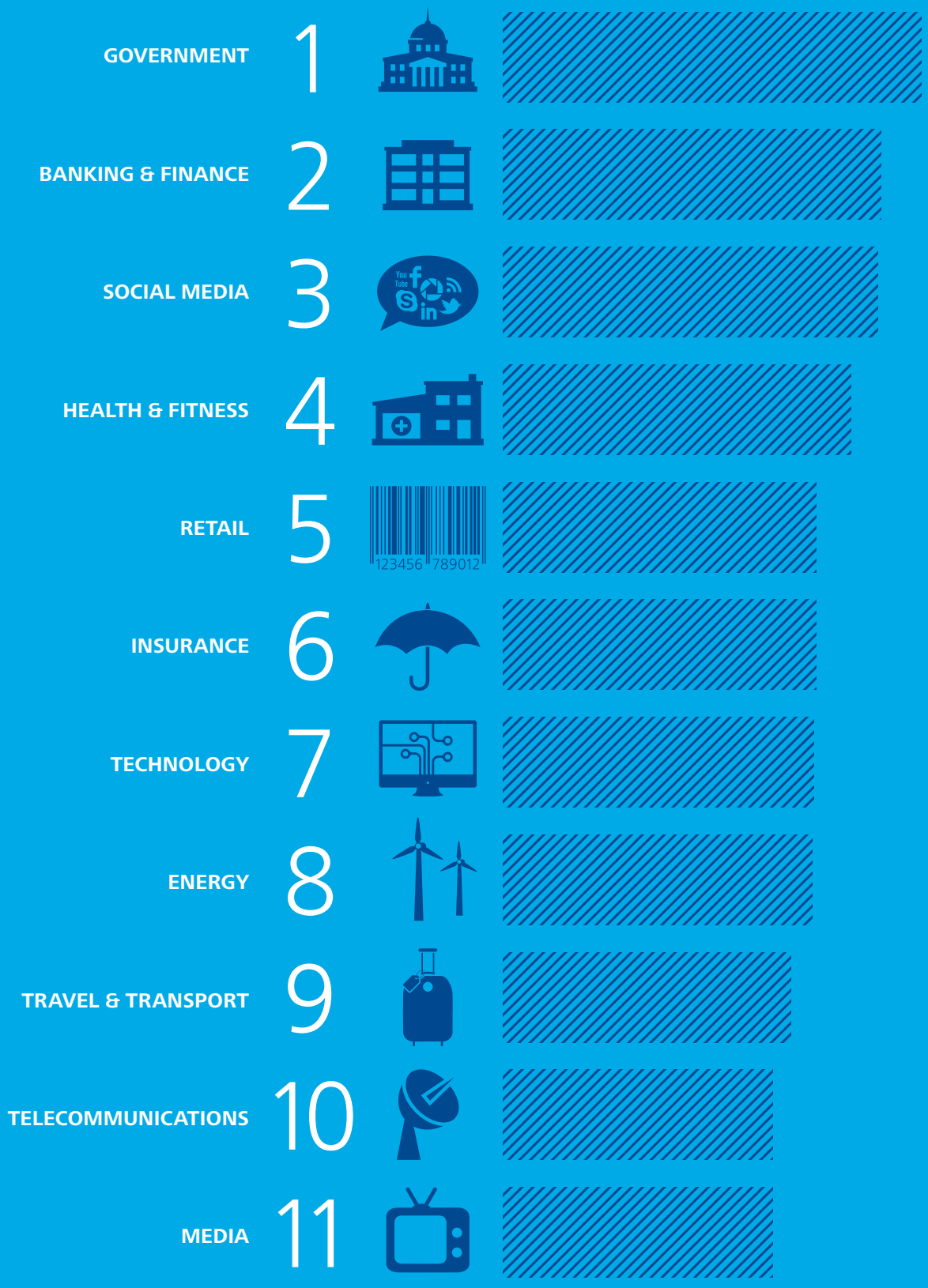
Thanks and acknowledgement

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

- All participating brands in the Deloitte Australian Privacy Index 2015 Survey
- David Batch.

[2]The source of mainstream online media was taken from the *Top Sites Ranked By Unique Audience For News* list provided by Nielsen: *http://www.nielsen.com/au/en/press-room/2015/nielsen-online-news-rankings-jan15.html.*
[3]User generated content included Facebook, Twitter, comments, blogs, images and videos.

Overall ranking of privacy performance across 11 industries



Executive summary

The Index reveals the overall ranking of 11 industry sectors.

It was compiled by aggregating the results drawn from the following three components that were assessed for each brand:

- Consumer sentiment
- Website
- Media sentiment.

The key themes identified were wrapped around transparency, regulatory change and governance.

Overall sector ranking

The list below indicates how industries performed across all areas assessed by the Index for being transparent – a key indicator of trust, having the best governance policies and procedures, and being up to date with current regulatory change. 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. Government
2. Banking & Finance
3. Social Media
4. Health & Fitness
5. Retail
6. Insurance
7. Technology
8. Energy
9. Travel & Transport (airlines, agencies, hotels, taxi)
10. Telecommunications (mobile, internet, home phone)
11. Media (news, television, radio, entertainment).

Key insights

- Government organisations were the clear leaders in privacy across all three components assessed, achieving four positions in the top ten
- Government and Banking & Finance organisations tended to have online policies with supporting material explaining different aspects of privacy
- Government organisation websites also had the lowest number of third party cookies
- The Banking & Finance sector dominated over half the top ten in the Index, with 70% of organisations in the Banking & Finance industry that were assessed appearing in the top 50% of the Index
- While consumer and media sentiment was low regarding Social Media, the Social Media sector performed strongly in the Index due to the transparency of its online policies and leaving the second lowest number of third party cookies on the device of a consumer, just behind Government organisations
- Sectors featuring in the lower half of the industry ranking tended to have a standard privacy policy online as well as a significant number of third party cookies.

Organisations that did well have

- An online privacy policy which is both easily understood by the consumer and layered, and often is supported with extra materials
- Have less third party cookies tracking consumer behaviour
- Cookies on their website which do not stay on the consumer's device for a long time
- A trusted brand according to consumers
- Few or no major privacy events reported in the media.

Consumer sentiment analysis

The top three most trusted industries as identified by consumers:

BANKING & FINANCE

GOVERNMENT

HOSPITALS

When asked to provide the three most sensitive types of personal information:

67% **CREDIT CARD**

46% **PASSPORT**

43% **DRIVER LICENCE**

Of the responses to organisations the public trust the least with personal data:

10% of the public said they did not trust anyone

52% indicated they were not current consumers of the organisation they did not trust

26% had never used the organisation they did not trust

Thought: How can organisations build trust through transparency to retain their customers?

Brand analysis

Most organisations have an internal privacy policy

Training is compulsory for all employees in all organisations which have privacy training. However, this training is done less than annually in most organisations

2/3

Over two thirds of organisations have a data breach policy

Thought: Is a compliance-only approach to privacy management sufficient? What can organisations do to manage privacy concerns amidst the current technology developments?

Media sentiment analysis

The top three performing industries in regards to media sentiment:

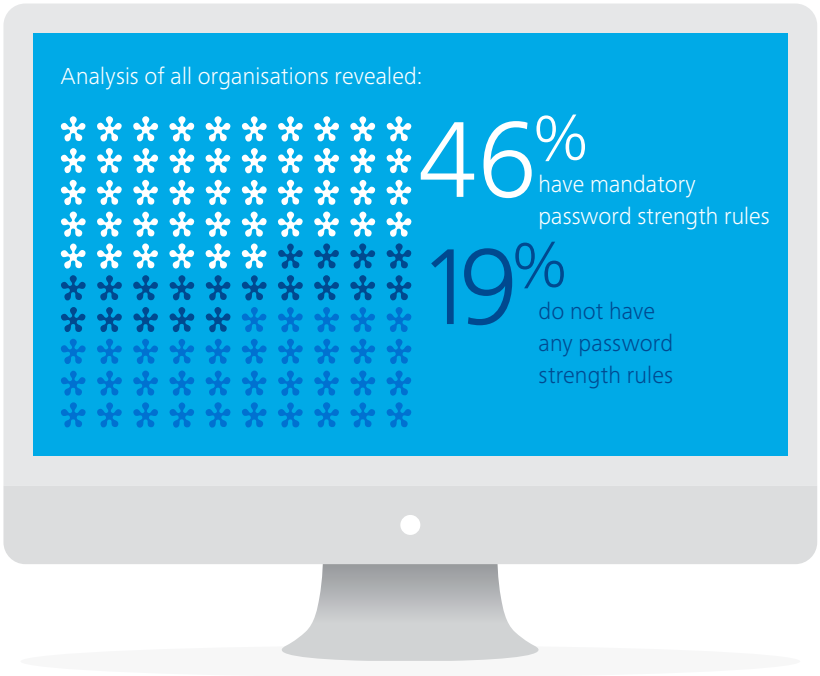
Thought: How can brands position themselves to obtain overall positive media sentiment?

Website analysis

Few organisations have implemented two-factor authentication.

The Banking & Finance industry were the best.

BANKING & FINANCE



Thought: Do consumers understand how their information is used when doing business with us online?

18%

OF SURVEY PARTICIPANTS HAD RECEIVED A PRIVACY NOTIFICATION FOLLOWING A LOSS OF PERSONAL DATA BY AN ORGANISATION

COMPARED TO

27%

WHO SAID THEY TRUSTED THEM LESS

OF THOSE

34%

SAID THEY TRUSTED THAT ORGANISATION MORE

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. Not all brands were mentioned in the consumer survey.

Industry ranking

The list below indicates how industries performed for the consumer sentiment component of the Index with the number one industry performing the best:

1. Government
2. Banking & Finance
3. Insurance
4. Energy
5. Travel & Transport (airlines, agencies, hotels, taxi)
6. Health & Fitness
7. Media (news, television, radio, entertainment)
8. Telecommunications (mobile, internet, home phone)
9. Retail
10. Technology
11. Social Media

Key insights

- Australian consumers are most concerned about their credit card details (67%), their passport number (46%), and their driver licence number (43%) being shared. Consumers are also most reluctant to share these three items due to their sensitivity
- Banking & Finance and Government are the top two most trusted industries when it comes to safeguarding personal information
- The Insurance industry is trusted less with personal information than Banking & Finance
- Overall 67% of the 1000+ consumers surveyed have never had a privacy issue with a brand
- The remaining 33% have had a privacy issue with an organisation, but only 14% have complained
- Social Media and the Telecommunications sectors accounted for 58% of the complaints regarding privacy. Social Media had 32% of the complaints.

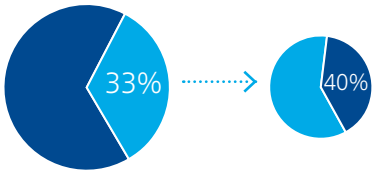
Looking at three main areas

Trust

- 14% of the public picked the same bank as their most trusted organisation
- In fact, five of the top ten most trusted organisations were banks
- 12% of the organisations selected as most trusted, were selected even though the respondee had not used them
- 28% of people listed the same social media organisation as the organisation they trusted the least with their personal information
- The two least trusted brands were in the Social Media sector
- Of the responses to organisations the public trust the least with personal data, 52% were not current users of that organisation's services (indeed more than quarter of respondents (26%) had never used that organisation)
- 10% of the public said they did not trust anyone
- Some consumers were suspicious of the survey and would not reveal who they do not trust. Comments included: 'I don't wish to name them', 'None of your business', and 'There are no organisations that I fully trust'.

Complaints

ONE IN THREE ORGANISATIONS HAVE HAD A PRIVACY ISSUE RELATING TO THE PERSONAL INFORMATION THEY STEWARD



OF THAT THIRD, AROUND 40% OF RESPONDENTS EITHER COMPLAINED TO OR ABOUT THE ORGANISATION/BRAND

- Social Media and Telecommunications sectors are those most identified with privacy issues by consumers
- Both men and women had complained equally
- We complain more about privacy as we get older: 4% of respondees aged 25 or under said they had made a privacy complaint vs. 16% of those over 40.

Notification

- 18% had received a privacy notification following a loss of personal data by an organisation
- Of the just under one fifth who responded they had been notified of a breach, 34% said they trusted that organisation more compared with 27% who said they trusted them less
- 73% of the public who received a privacy breach notification did not trust the organisation any less following the notification.

Organisations that did well

- Are in industries with clear regulations on how information should be handled
- Supply the most sensitive information to consumers such as password information and credit card details
- Notified their customers of any data breaches that occurred leading the customers to trust these organisations more
- Had less privacy complaints.

Over half of the organisations surveyed conduct Privacy Impact Assessments

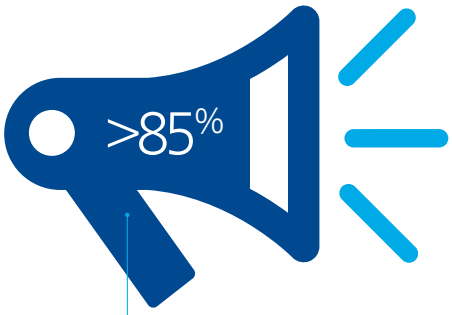
Brand analysis

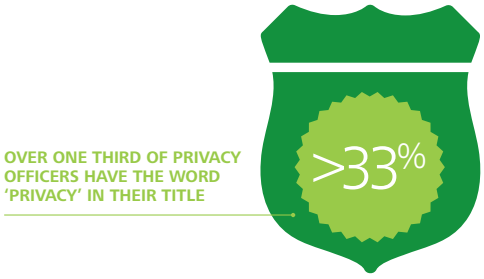
Privacy capabilities within organisations are maturing. Deloitte analysis was performed on leading consumer brands to measure the maturity of privacy management within their organisation.

Key insights

- More than 75% of organisations indicated that there is a privacy officer role within the organisation. Over one third of these privacy officers have the word 'privacy' in their title. Of these appointments, 75% manage privacy for the organisation full-time
- Most organisations have a customer-facing privacy policy and those with one, make it available online. Most organisations also have an internal privacy policy
- Training is compulsory for all employees in all organisations with privacy training. However, this training is done less than once a year in most organisations
- More than two thirds of the organisations surveyed have a data breach policy, with less than half committed to training their staff in this policy
- Over half of all organisations notified their CEO of all data breaches in the last 24 months. More than 85% notify the person in charge of risk for the organisation, of data breaches
- More than half of the organisations surveyed conducted Privacy Impact Assessments in the last 12 months
- Of the organisations that have conducted at least one Privacy Impact Assessment, 60% have completed more than five assessments
- More than half of the organisations surveyed have an ethics policy or values statement that specifically refers to privacy.

The brand assessment was not considered for the industry ranking as Deloitte was unable to verify the answers provided. However, useful insight was 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.





Few organisations list the specific countries in which information may reside, but rather make a generic comment that information may be transferred overseas to third parties or the like.

Website analysis

The website analysis of the brands involved assessed their online privacy policy and the cookies the website stores on the devices of visitors to the website.

A **first party cookie** enables the website of an organisation to create a more seamless user experience. The organisation is the owner of this type of cookie.
A **third party cookie** is used by an organisation to track consumer preferences online. The organisation is not the owner of this type of cookie. The third party cookie will store the information about the consumer's actions when using the organisation's website.
A **session cookie** is set on a consumer's device by a website until the web browser is closed.
A **persistent cookie** is set on the device by a website with an expiry date. When that expiry date is reached, the cookie is removed from the consumer's device.

Industry ranking

The following list indicates how industries performed against the parameters of the website component of the Index. With the number one ranked the best:

1. Social Media
2. Government
3. Technology
4. Health & Fitness
5. Banking & Finance
6. Energy
7. Insurance
8. Telecommunications (mobile, internet, home phone)
9. Travel & Transport (airlines, agencies, hotels, taxi)
10. Media (news, television, radio, entertainment)
11. Retail

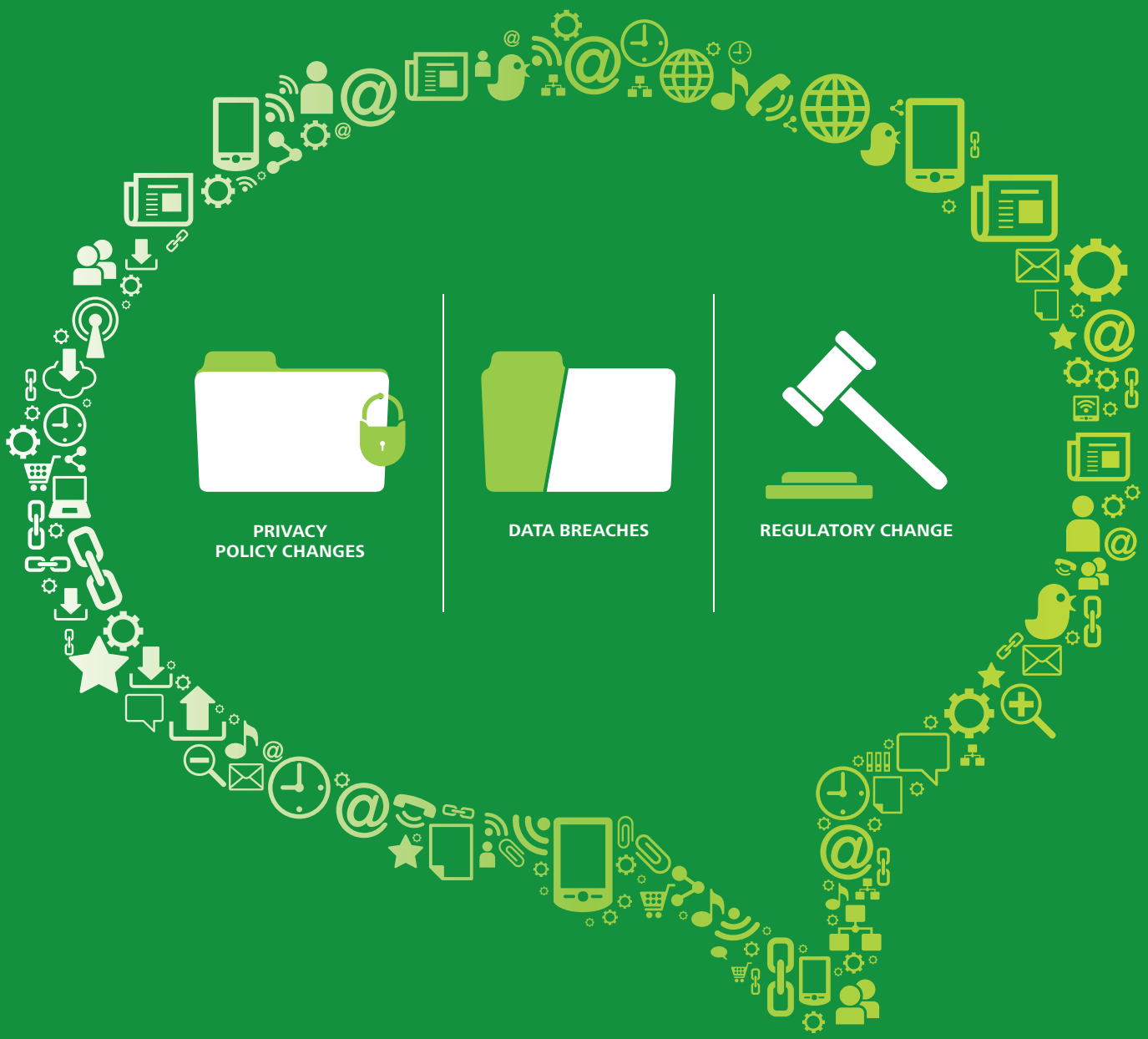
Key insights

- Social Media has attracted the highest score. Social Media privacy policies tend to be transparent, user friendly and have supporting materials which educate consumers on how to use their services. It is also the industry using the least third party cookies
- Few organisations list the specific countries in which the data they hold may reside but tend to make a generic comment that data may be transferred overseas to third parties or the like
- Social Media and Government organisation performed equally strongest in the cookie analysis. Both industries have the lowest number of third party cookies
- Social Media has the shortest average duration for a third party cookie stored on a consumer's device
- The Telecommunications and Retail industries both had a third party cookie which would be stored on a device for more than 135 years when a consumer visited their website
- The Retail industry places the most cookies on a consumer's device in general, followed closely by Banking & Finance. The Retail industry also has the highest average number of third party cookies. It also had the highest average duration for which those cookies would be stored on a visitor's device
- The Retail industry did not tend to make supporting material available on their websites to assist consumers to understand their privacy policy. Most don't specify the countries to which customer information may be sent
- The average length of time cookies are stored on a device across all brands is 777 days – that is more than two years
- The Health & Fitness and Energy sectors have the highest average number of cookies stored on a device, followed by telecommunications organisations
- Few organisations have implemented two-factor authentication (this typically is where you have an additional login code that is taken from something you have). The Banking & Finance industry were the best
- Just under a half of the brands analysed (46%) have mandatory password strength rules. However almost a fifth of those surveyed (19%) did not have any password strength rules at all
- 74% of organisations educate consumers visiting their website about cookies and how to remove them
- Less than 4% of brands actively notify consumers the first time the home page of their website is visited, that cookies are being installed on their devices
- Technology, Social Media and Telecommunications firms operating in Australia tend not to make reference to the Australian Privacy Principles
- The Media sector had the highest percentage of cookies files remaining on a device after closing a web browser (known as persistent cookies).

Organisations that did well:

- Had online policies which were layered
- Listed the countries in which information could travel
- Had supporting materials to assist consumers in understanding their policy e.g. a video
- Had the least number of third party and persistent cookies
- Placed cookies on devices for a short duration.

The top three key themes gleaned from the articles



Media sentiment analysis

Media sentiment of privacy across the brands was assessed across mainstream online media and user generated content as either positive, negative or neutral. Not all brands assessed were mentioned in media.

Industry ranking

The list below indicates how industries performed for the media sentiment component of the Index with number one the most positive and 11 the least:

1. Insurance
2. Energy
3. Banking & Finance
4. Health & Fitness
5. Retail
6. Travel & Transport (airlines, agencies, hotels, taxi)
7. Government
8. Media (news, television, radio, entertainment)
9. Telecommunications (mobile, internet, home phone)
10. Social Media
11. Technology.

Key insights

- More than 42% of the brands assessed had positive or negative sentiment relating to privacy across mainstream online media and social media
- Media sentiment favoured the Insurance industry followed by Energy and then Banking & Finance
- The Technology and Social Media industries faired least favourably
- With mainstream online media, the Health & Fitness industry performed the best, with the Technology, Media and Social Media sectors performing the worst
- For user generated content: the Banking & Finance and Insurance industries performed the best, and the Media industry the worst.

Key themes in the media

- Privacy policy changes have featured in the media both positively and negatively
- Data breaches that large consumer brands suffered
- Concern around the increased capabilities of technology devices
- Regulatory changes proposed in Australia such as data retention and mandatory data breach notifications
- Organisations with a public data breach that have made changes to policies or internal practices, faired positively in the media.

Organisations that did well

- Have not had a major reported event such as a change in privacy policy, or a data breach
- Have taken remedial action such as changing policies where there has been a major reported event.

Forward thinking and actively managing privacy risk are essential to understanding and acting on your privacy responsibilities. Simply maintaining the status quo, whether in relation to a data breach, or in relation to the changing landscape of data protection and information handling, is the most ineffective way of dealing with the challenges of the information age. Privacy leadership, and from this, a robust culture of accountability and governance, is the most effective way of rising beyond mere box-ticking compliance to best practice.

Timothy Pilgrim, *Australian Privacy Commissioner*, 'Privacy Governance' (Speech delivered at the iAPP ANZ Forum, Sydney, 11 February 2015)

Future trends

Privacy has been a hot topic over the past 18 months within Australia following the Government's recent privacy changes in March 2014. This has created a lot of positive focus as organisations look to comply with the updated requirements. Just over a year on from this update, is a 'compliance only' approach enough given current technology developments?

Notifying customers of data breaches

The survey results show that consumer trust is built through transparency. This is especially pertinent given the discussions the government is currently having regarding mandatory data breach notifications. Organisations can begin positioning themselves by implementing a governance framework to monitor and measure how information is used. This includes:

1. Understanding what information is collected and disclosed.
2. Understanding where and how information is held. For example, information can be held both in key systems as well as extracted in various forms and transferred internally or externally to third parties.
3. Vigilance as to what activities are performed with the held information, including monitoring suspicious or abnormal behaviour, so you can block or know early if a potential breach is to occur.
4. Having a well-known and effective response plan. Once individuals know and practice their role, the response to a breach becomes like 'muscle memory'. Practicing this through realistic simulations is critical.
5. Consumers will become more familiar with data breaches. As more breaches are reported and consumers expect speedier notification, they also expect the detail of the information shared to increase.

Big data insights versus consumer ethics

Deriving new insights and opportunities from an organisation's available data, is an important focus for many organisations. However, when does that intelligence go too far in terms of what a consumer would reasonably expect, based on the original information they provided?

This conundrum will continue to attract differing opinions from those who find it helpful and welcome the insight, to those who feel the interest goes beyond the 'creepy line' and becomes intrusive.

A valuable challenge and test of planned and newly derived insights comes back to ethical considerations.

1. Is the organisation transparent about what it does with this information?
2. Is this communicated in simple language internally and placed somewhere where it can be easily referenced?
3. Would an individual reasonably expect you to use the information you have in the way that you do use it?
4. Does the derived information conflict with any of the organisation's key values or strategy?

Organisations will continue to use data analytics to advance their strategic goals, but the ones with effective business strategies will embrace privacy as a driver of creativity and innovation, and embed it into their systems to ensure quality results.

Beth Dewitt, *Senior Manager and Privacy Specialist* in Enterprise Risk Services, Deloitte Canada

Personalisation

Personalised user content is not that new. It is something that has, and will, continue to grow as organisations draw deeper insights into user behaviour. What our research showed was the number of third parties organisations are relying on in an attempt to achieve optimum personalisation.

In our view this will only continue when driven by the benefits an organisation receives, in targeting the interests of a current or potential customer. This practice can be extremely valuable to individuals, but needs to be transparent so people know how their actions with an organisation will be tracked and used.

Privacy compliance to privacy by design

Many organisations have worked towards complying with the updated privacy requirements. However, a pure compliance approach may be risky. A better way to meet privacy requirements over the longer term is to embed privacy into everything an organisation does, so that privacy considerations are included by design.

This would require creating a set of organisational privacy principles, and performing privacy impact assessments as part of any new business change impacting personal data. This would mean restricting those on a project with access to personal data, or for example, building in the necessary functionality to enable customers to make a choice regarding how their information is used, such as opting into certain communication types.

Key to this process is that individuals within the organisation understand the basic privacy requirements, and critically, know where to go when they have a question.

Getting the privacy basics right

Many data breaches are avoidable. Despite a steady increase in serious cyber-attacks, the vast majority of reported data breaches involve accidental loss or release of data, communications being sent to the wrong person, missing basic security controls and a lack of training and awareness of staff. These are some of the most frequent causes of data breaches and with the proper checks and balances, and policies and procedures in place are largely preventable.

Organisations must try to be at least in a position to justify the preventative measures they have taken, so that if they were to have a data breach they are able to confidently say, they took reasonable action to prevent and manage a breach.

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)
Healthcare Identifiers Act 2010 (Cth)
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 which contain privacy requirements.

Other references

Casper, Carsten, 'Hype Cycle for Privacy, 2014' *Gartner, Inc* (18 July 2014)

Deloitte Australian Privacy Index: *http://www2.deloitte.com/au/privacy-index*

Deloitte Cyber Security: *http://www2.deloitte.com/au/en/pages/risk/solutions/cyber-security.html*

Nielsen, *New Year, New You: Nielsen Online Ratings for January show Seasonal Spikes in People Accessing Lifestyle-Related Sites* (11 February 2015): *http://www.nielsen.com/au/en/press-room/2015/nielsen-online-news-rankings-jan15.html*

Office of the Australian Information Commissioner ("OAIC"): *http://www.oaic.gov.au*

Timothy Pilgrim, 'Privacy Governance' (Speech delivered at the iAPP ANZ Forum, Sydney, 11 February 2015): *http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-governance*

With greater personal information comes greater responsibility. As organisations consume more data from their users directly and indirectly to provide customised online personalisation and other valuable insights, there is an increased need and expectation for transparency, security, ethical use and overall governance around personal data. This would mean, that as well as organisations deriving benefit, users are kept informed of the use and key changes to their data.

Gavin Cartwright, Cyber Risk Services, Deloitte Australia

Deloitte Australian Privacy Index 2015

The table below indicates the ranking of all brands assessed for the purpose of the Index. The industry of the brand is shown rather than the brand itself.

Rank	Brand industry
1	Government
2	Banking & Finance
3	Banking & Finance
4	Government
5	Banking & Finance
6	Banking & Finance
7	Banking & Finance
8	Government
9	Social Media
10	Government
11	Banking & Finance
12	Banking & Finance
13	Social Media
14	Banking & Finance
15	Banking & Finance
16	Energy
17	Retail
18	Energy
19	Telecommunications (mobile, internet, home phone)
20	Energy
21	Health & Fitness
22	Energy
23	Retail
24	Insurance
25	Media (news, television, radio, entertainment)
26	Government

Rank	Brand industry
27	Retail
28	Banking & Finance
29	Technology
30	Technology
31	Banking & Finance
32	Retail
33	Government
34	Media (news, television, radio, entertainment)
35	Government
36	Social Media
37	Travel & Transport (airlines, agencies, hotels, taxi)
38	Telecommunications (mobile, internet, home phone)
39	Energy
40	Retail
41	Banking & Finance
42	Insurance
43	Insurance
44	Banking & Finance
45	Health & Fitness
46	Health & Fitness
47	Technology
48	Government
49	Banking & Finance
50	Banking & Finance
51	Retail
52	Retail

Rank	Brand industry
53	Retail
54	Technology
55	Media (news, television, radio, entertainment)
56	Travel & Transport (airlines, agencies, hotels, taxi)
57	Banking & Finance
58	Insurance
59	Health & Fitness
60	Media (news, television, radio, entertainment)
61	Travel & Transport (airlines, agencies, hotels, taxi)
62	Telecommunications (mobile, internet, home phone)
63	Media (news, television, radio, entertainment)
64	Technology
65	Insurance
66	Insurance
67	Health & Fitness
68	Social Media
69	Travel & Transport (airlines, agencies, hotels, taxi)
70	Social Media
71	Banking & Finance
72	Telecommunications (mobile, internet, home phone)
73	Travel & Transport (airlines, agencies, hotels, taxi)
74	Government
75	Health & Fitness
76	Travel & Transport (airlines, agencies, hotels, taxi)
77	Travel & Transport (airlines, agencies, hotels, taxi)
78	Travel & Transport (airlines, agencies, hotels, taxi)

Rank	Brand industry
79	Banking & Finance
80	Energy
81	Health & Fitness
82	Insurance
83	Telecommunications (mobile, internet, home phone)
84	Telecommunications (mobile, internet, home phone)
85	Retail
86	Travel & Transport (airlines, agencies, hotels, taxi)
87	Retail
88	Media (news, television, radio, entertainment)
89	Insurance
90	Retail
91	Technology
92	Retail
93	Banking & Finance
94	Retail
95	Travel & Transport (airlines, agencies, hotels, taxi)
96	Media (news, television, radio, entertainment)
97	Travel & Transport (airlines, agencies, hotels, taxi)
98	Retail
99	Technology
100	Insurance
101	Banking & Finance
102	Media (news, television, radio, entertainment)
103	Telecommunications (mobile, internet, home phone)
104	Energy

Contacts

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

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

Sydney
Gavin Cartwright
Cyber Risk Services
+61 2 9322 3580
gavcartwright@deloitte.com.au

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

www2.deloitte.com/au/privacy-index

MCBD_SYD_04/15_051593