Deloitte.

The Symbiotic Relationship

Getting the balance right

Deloitte Australian Privacy Index 2018

"The success of an organisation that handles personal information, or a project that involves personal information, depends on trust. People have to trust that their privacy is protected, and be confident that personal information will be handled in line with their expectations."

Timothy Pilgrim, Australian Privacy Commissioner,
'Commencement of the Notifiable Data Breaches scheme',
Thursday, 22 February 2018

Contents

Introduction

As technology, consumer demands, and business models continue to evolve, brands are collecting vast amounts of personal information, which exponentially increases year-on-year.

Each brand will use this personal information differently. Some will commoditise it, others will use it to create a more customised experience. In either case, transparency with the consumer on how their personal information will be used and protected is critical. Honest communication on which data is being used for what, will become essential for any continued value exchange.

Deloitte Privacy Index 2018

In our 2018 Deloitte Privacy Index we examine how the top 100 brands in Australia currently communicate what they are doing with their customers' personal information and how they feel about it. We then rank those brands by sector. And in the interests of building a resilient and sustainable Australia we list some ways privacy practices can be better communicated and executed.

The symbiotic relationship

The terms 'symbiosis' or 'symbiotic' are not commonly used in business to describe the relationship between consumers and the brands they seek goods and services from. However, we at Deloitte believe that this term quite simply explains the co-dependent types of relationships that can exist between the parties.

In the business 'ecosystem' that exists between consumers, brands and the products and services they create, there is almost always a personal information value exchange that requires careful balance between all parties to survive and thrive. Such an exchange needs to be of mutual benefit, growing together through a long and fruitful relationship.

This is where most brands strive to be in a consumer's lifecycle. Symbiosis of mutual benefit.

The opposite of mutualistic symbiosis is parasitic symbiosis, the kind that can be devastating to an ecosystem's sustainability when one side over exploits the other. This is analogous to a brand that collects personal information at all costs, ignores the reputation and trust impacts, and ultimately destroys the relationship with its consumers, whilst also undermining the broader digital economy with it.

Today, consumers are providing increasing levels of personal information in return for services and benefits. They have trusted those brands to use this information for the purpose they supplied it. Given the increasing awareness of broken promises across multiple sectors, from sport, through social media, to finance, this trust will now need to be earned.

The danger signs are there. And given the fact that most consumers do not read privacy policies, yet have significant expectations as to how their data is used and shared, there is a big gap between expectation and reality.

The media's daily exposés of where trust has broken down are triggering detailed investigations and exposure as to how personal information is collected, used, shared or created across multiple service providers. The results are leaving many consumers feeling uncomfortable and exposed. This cannot be a positive for the brands involved, especially as business relies on trust. The business and innovation opportunities for those that get their trust positioning right will be significant.

Tommy Viljoen
National Lead Partner
Cyber Risk Services,
Risk Advisory

David Batch
National Privacy and Data Protection Lead,
Risk Advisory

About this report

The 2018 Deloitte Australian Privacy Index focuses on privacy practices regarding personal information collection, use, disclosure and retention by organisations and their brands, and the sentiments of consumers to these practices.

Participating in this year's surveys were more than 1000 Australian consumers, and leading brands that operate in the Australian market across 10 industry sectors.

We also analysed the publicly available statements that brands make regarding their privacy and personal information handling practices.

Consumer sentiment analysis

The survey captures the attitudes and opinions of more than 1000 Australian consumers, aged 18 and above from all regions who were asked to state how they understood the nature of their personal information exchange with brands in return for goods and services.

We asked these consumers what data they provided to the brands and what factors influenced their decision to share their personal information. The focus was to understand the trust relationship and what factors influence the increase or decrease of consumer trust in brands.

We also asked consumers to consider their knowledge of privacy, how they would feel if their data was involved in a breach and what their expectations were for the brands to respond to such incidents.

Brand analysis

This report combines the findings of a brand survey, completed by representatives from leading Australian companies with research findings that examine publicly disclosed privacy practices of 100 leading brands in 10 industry sectors. Combining these insights we have developed an Index ranking each of those 10 sectors.

This year's survey of the top brands focuses on the maturity of their internal privacy practices.

The survey collected information about brand capabilities such as the role of their privacy function, its responsibilities, processes and how privacy awareness initiatives are managed. We collected this information from Chief Privacy Officers, Chief Risk Officers and employees responsible for privacy, legal, risk and brand.

Results

All responses to these surveys are confidential and anonymised. This index reports only aggregate responses, statistically analysed and visualized throughout the report to provide insights into the state of privacy.

Acknowledgements

We would like to acknowledge following for their support:

- All participating brands and consumers in the Privacy Index 2018 surveys
- Roy Morgan Research Ltd for conducting the consumer survey on behalf of Deloitte
- The Deloitte Risk Advisory Team led by Vikram Asnani, supported by Maha Arif, Margaret Austen, Michele Bahari, Marie Chami, Divya Jamdagni, Sebastian Le Cat, Esther Lim, Pauline Pang, Ilana Singer and Jasmin Wong
- Partners who assisted with the brand survey.

Executive summary

As the relationship between brands and consumers constantly evolves, brands have to amend their privacy practices to meet both consumer expectations and regulatory change. The increasing emphasis on consumers 'owning and having control over' their data is a seismic change to the status quo.

This year's Deloitte Privacy Index results clearly establish that trust and transparency play a vital role in determining the strength of any potential symbiotic relationship between the brand and its consumers.

Key themes

- Transparency of personal information use and disclosure will be key to building trust as consumers become more aware of their privacy rights.
- Consumers are willing to share their personal information with brands for a clear benefit.
- Disclosure of personal data to third parties that consumers haven't consented to decreases trust.
- Transparency regarding personal information incidents and breaches is an opportunity to build trust.

Key insights

- Consumers are expecting greater control of their data before they are willing to share it with brands.
- Companies that have information processing at their core, such as online businesses and those in the information technology sector, demonstrate a greater understanding of privacy compliance and best practice.
- Clear and transparent notices regarding data use go hand in hand with consumer trust and willingness to share their personal information.
- Consumers lose trust in companies which use their personal information in ways not explicitly agreed to, such as marketing.
- 69% believe that trust in, and the reputation of the brand is most important when making a decision about sharing personal information, followed by the benefits received, such as discounts, personalised service and rewards.
- Brands are more likely to lose consumer trust and damage their reputation if customer data is used for direct sales (68%), inappropriate marketing (58%) and cross-selling of personal information (54%).
- Consumers are aware that their personal information may be shared with third parties and 41% are comfortable allowing a brand to transfer their data if they trust the brand and there's a benefit in doing so.
- Despite the notifiable data breach requirements under the 1988 Privacy Act recently coming into effect and receiving considerable media attention, 58% of consumers are unaware of these new requirements. However, 90% of consumers still expect to be notified if their personal information is involved in a breach.
- Brands can retain customers and gain trust if they respond to breaches quickly and effectively. 76% of respondents indicated that they would be more likely to trust a brand after a breach if there was timely notification of the breach, a detailed explanation of the breach, detailed remediation plans, and ongoing notifications on progress.

Overall sector ranking

- This year's Index ranked the sectors as follows:
  1. Information Technology
  2. Finance
  3. Government
  4. Telecommunications and Media
  5. Travel and Transport
  6. Retail
  7. Real Estate
  8. Health and Fitness
  9. Education and Employment
  10. Energy and Utilities
- Given the focus on transparency of personal information processing there was significant shift in sector ranking over previous years.
- Brands that offer primarily digital goods and services ranked better on transparency measures.

Five things to ensure an effective, transparent symbiotic relationship

1. Be upfront

You're good at marketing the consumer benefits of sharing data; become good at including the benefits you obtain in that communication. Do this before you collect a consumer's personal information. Footnotes, links to and off-site references can seem like you are trying to hide something.

2. Ensure your privacy policy is concise, direct and follows the OAIC guidelines

Too many privacy policies are missing key transparency elements and are legalistic, vague and difficult to understand. The consumers who do take the time to read your policy are probably most likely to exercise their rights. Look at ways to be more direct and explore other ways to deliver the message, like a video or layered notices.

3. Don't rely solely on your privacy policy or terms and conditions

Consumers have indicated that they are unlikely to read these, so explore other options for communicating your plans for personal information use in order to maintain trust.

4. Be clear how you will use personal information

Using vague or high-level terms can be misleading. Be clear on what, where, when and how a customer's personal information will be used.

5. Develop an internal data retention and destruction policy and procedure

Many companies are unable to be clear about how long they will hold a consumer's data and whether it will be destroyed or permanently de-identified. This is typically because there is no internal policy or procedure to help define this. Once internal data retention policies and procedures are developed, these will enable consumer facing privacy policies and other communications to be clear about how and when data will be retained and destroyed.

Privacy Index 2018: How each sector ranked

Sector	Rank 2018		Rank 2017		Rank 2016
Information Technology	1	↑	9	↓	7
Finance	2	↓	1	→	1
Government	3	↓	2	→	2
Telecommunications and Media	4	↓	3	—	N/A
Travel and Transport	5	—	N/A	—	8
Retail	6	↑	7	↑	10
Real Estate	7	↑	8	↑	13
Health and Fitness	8	↓	6	↓	4
Education and Employment	9	↑	11	↓	6
Energies and Utilities	10	↓	4	↓	3

↑ Ranking Increased ↓ Ranking decreased → No change in Ranking

This year's research and findings centre on the theme of transparency and as such there has been some large movement in the Index ranking over previous years.

The brand sectors that made more effort to communicate their privacy practices with consumers in a transparent way scored higher than those that did not. It is important to note that this is not an Index on how actual personal information processing activities matches up with what is disclosed by each brand (which is difficult to accurately measure without audit-level insider information).

Each brand that was surveyed had an online presence, however a key observation when considering the scores of each was that those whose product or service offering was primarily in the digital space typically scored higher than those that did not, suggesting a greater understanding of privacy and privacy regulatory requirements. Given some sectors have been more disrupted than others in the digital space, this may explain the shift in movement. More detailed findings on this can be found in the Brand Analysis section.

Brand analysis

There have been some significant and recent high profile issues capturing the world's attention that centre around large scale unethical, if not unlawful, personal information use and disclosure that have enraged consumers across the globe. The media and political attention these have received are sure to be keeping corporate board members, CEOs and in-house privacy professionals awake at night wondering 'Will we too be publicly called to account for our personal information handling practices?', 'Exactly what personal information do we have?', 'How did we get it?' and 'Have we used it lawfully?'.

For some time, the main focus of media and corporates when considering privacy has been on data security. Large-scaled data breaches that get the attention of the media are usually linked to criminal activity which is innately intriguing and sensational. But while security of information is critical to maintaining privacy, the issue of privacy is much larger than 'how good is your fence and how secure is your gate?'

2018 is turning out to be a landmark year in terms of the biggest privacy incidents of all time, especially considering the impact the alleged misuse of personal information has had on the companies involved, the broader share market and geopolitics, the number of people affected, and the sheer volume of personal information involved.

It is likely that many impacts are yet to be realised, especially in form of regulatory response. Central to these breaches is the fact that they have occurred not because of security lapses but because of information handling procedures that were at best poor and often at worst, planned and approved.

These incidents centre squarely around questions of lawful and ethical personal information collection, use, disclosure and retention. Key in this list is the broad term 'use'. How a company uses personal information is increasingly key to the value exchange that occurs between a consumer and the brand, especially where a brand intends to commoditise that information. How a brand uses that information is critical to the trust relationship with its consumers.

To determine if the personal information ecosystem is in good health, and the symbiosis between consumers and brands is balanced for mutual benefit, we have cross referenced findings from our brand and consumer sentiment research with analysis of the publicly available privacy practices of those brands, delivering the following key insights.

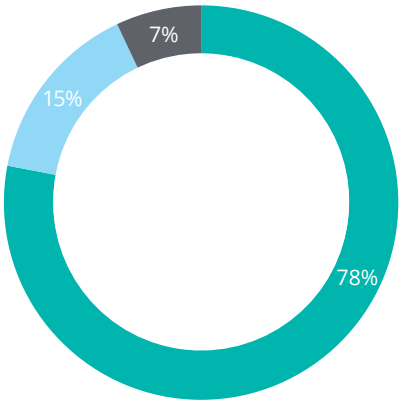
Key insights

Data Collection

There is a large variety of personal information that organisations use in order to do business and this data is collected directly from consumers, from third parties or created by the organisations themselves - but do they do a good job of being transparent about what data it is?

Of the organisations that we studied, 78% provided an exhaustive list of the types of data that they intend to collect from consumers. This high level of transparency and clarity demonstrates Australia-wide good practice, and enables consumers to develop a strong understanding of practices regarding how their data is collected.

Are major types of data collected specified?



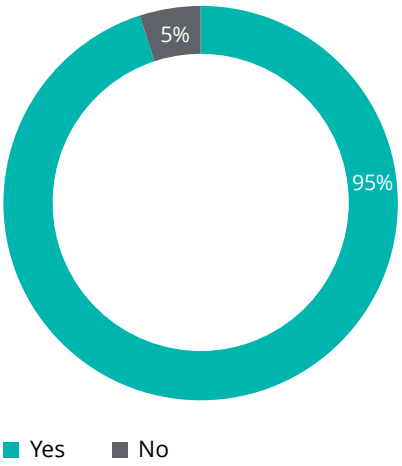
Sector-wise, government performed the best in this area, with each government department studied including data collection information.

This was closely followed by the finance sector. Conversely, just 50% of organisations in the education and employment sector were clear about what data they were collecting in their privacy policies.

Data Use

The use of data that consumers provide is at the core of the value exchange that consumers and organisations take part in. As such, for consumers to evaluate this exchange effectively and make informed decisions about where to provide their data, a high level of transparency is required of brands. Of the brands that we analysed, a healthy 95% had a section in their privacy statements referencing how they use the personal information that they collect from consumers.

Companies with data use sections

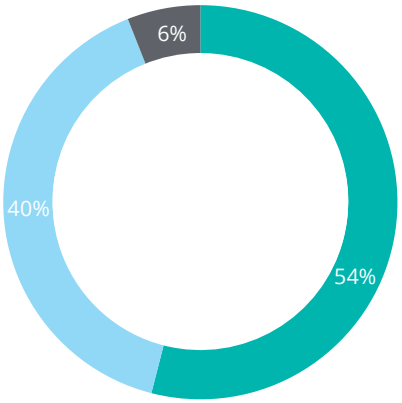


Most made some attempt to list key purposes for data use, with 54% of studied brands specifying a reasonably exhaustive list of major purposes for which consumer data was used within the business.

However, for 40% of brands this section was fairly vague and did not provide a sufficient amount of clarity for consumers to understand what key processes their data would be involved in.

On a sector basis, finance, energy & utilities and real estate scored very low on this particular topic with an average of under 50%.

Are major uses of data specified?

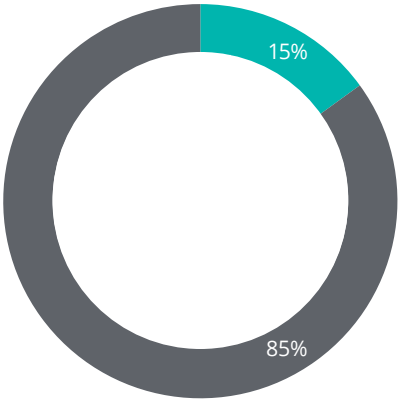


- Exhaustive list
- Small list and unspecified other uses
- None

While identifying the purposes personal information may be used for in privacy policies was the norm, far fewer brands elected to demonstrate how they would not use personal information. This addition to privacy policies and elsewhere in their interaction with consumers provides a very clear understanding of the boundaries that won't be crossed by the brands (e.g. by expressly stating data will not be provided to third parties for marketing).

Whilst not required as part of a public statement, stating what a brand won't do with personal information can provide an extra layer of assurance to consumers that their data won't be misused. It is therefore striking that just 15% of the organisations provide information on how they will not use personal information in their publicly disclosed privacy statements.

Privacy statements that specify how they won't use personal information?



- Yes
- No

The information technology sector (50%) and the telecommunication and media sector (29%) were most likely to include this information.

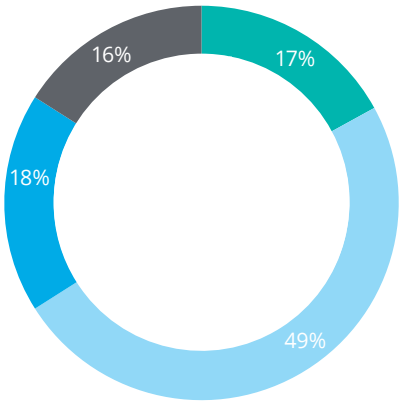
Data Disclosure

Another area of examination was how data was disclosed to third parties.

The majority of companies displayed good transparency in this area, with 17% of companies offering a reasonably exhaustive list of the countries that they disclosed data to. 49% specified certain jurisdictions but also indicated that data could be sent elsewhere offshore. 18% of companies merely identified that data would be sent offshore.

16% did not address third country disclosure, indicating that neither they nor suppliers were sending data offshore. A question arises here – 'Are brands failing to meet their compliance requirements for offshoring disclosure? Or are organisations and their third party vendors truly keeping all personal information within Australia?' Given the relative size and complexity of the 100 brands assessed, this figure is likely to indicate a lack of compliance with these requirements.

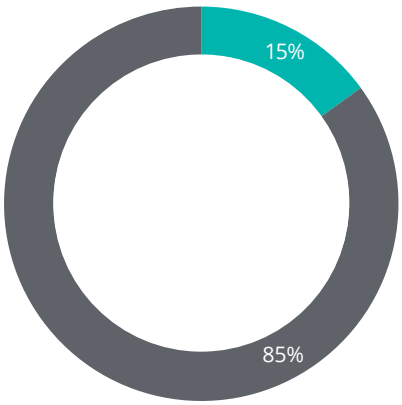
What countries does the third country disclosure section list?



- Small list and unspecified other countries
- Offshore
- Exhaustive list
- None

Across most sectors, organisations that indicated they were sharing data with third parties were not clear on whether such sharing was for third party marketing. Only 15% of brands expressly indicated they may share data for third party marketing purposes.

Do they provide third parties with data for their marketing purposes?



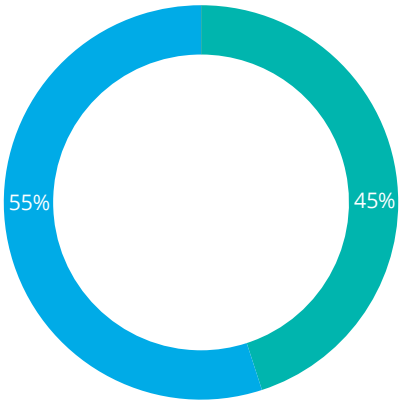
The retail, telecommunications and media and travel and transport sectors were more likely to indicate that they may be sharing data with third parties for marketing purposes, however the incidence of this was low at 30% in each of these combined sectors.

Data Retention/Deletion

The purpose of data sharing and participating in this value exchange, from a consumer perspective is to receive a service offered by an organisation, whilst the organisation uses this data to provide it. As such, when a consumer decides that they do not want to make use of the service/benefits anymore or the organisation has made use of the data for the purpose it was given, it can be expected the organisation will delete their data.

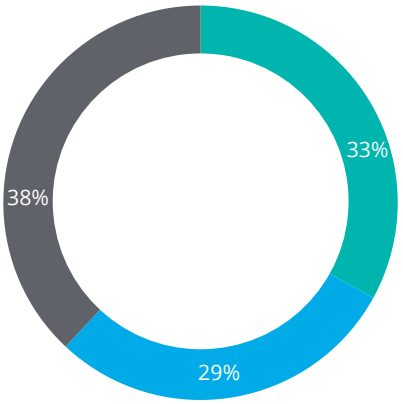
Specifying retention terms is therefore an important element for organisations to include in their privacy policy. Of the companies we surveyed 55% have referenced data retention in their privacy policy.

Do they have a retention/deletion section in their policy?



Of the companies that included a reference to data retention/deletion, 33% provided some specific details around time frames for retention and processes for deletion and 29% provided a basic outline of data retention practices. 38% of those who referenced retention and deletion did not give any further detail in regards to their practices.

How specific is their retention/deletion policy?



The finance sector scores best here, with more than 70% of the organisations having a specific data retention section included in their privacy policy and 50% defining when personal information will be deleted or permanently de-identified. It is not surprising that the financial sector excels here given its processing of highly confidential and valuable personal information and given it is subject to a stricter, multi-pronged regulatory regime.

The health and fitness sector scored particularly low on this metric, where just over 20% included data retention provisions in their privacy policy and just 5% defined when personal information would be deleted or permanently de-identified.

Digital vs non-digital businesses

The research showed differences between companies that conduct their business mostly in the digital or non-digital spaces. Digital companies provide more detail on personal information handling practices in their website privacy policies than non-digital companies. Given a company website has all but become the standard for where to find comprehensive information on its brand's privacy practices, the latitude perhaps given by regulators and consumers for this divergence, if any, will likely decrease over time.

Within sectors the difference between digital and non-digital operators becomes even more clear. Within the real estate sector only 71% of the non-digital companies are clear about the personal information that they are collecting against almost a perfect score for the digital companies we examined.

What is even more striking is that just 20% of the non-digital organisations within the education and employment sector are clear about their personal information collection practices against almost a perfect score for the digital companies.

Within the travel and transport sector 33% of non-digital businesses included a personal information retention section in their privacy policy against 75% of the digital businesses.

67% of the digital businesses within the telecommunications and media sector provide guidance on when and how data is permanently destroyed or de-identified against just 14% of the non-digital businesses.

In the end the digital companies score an average of 71% greater compliance with the legal requirements and best practice elements we considered against 65% for non-digital companies.

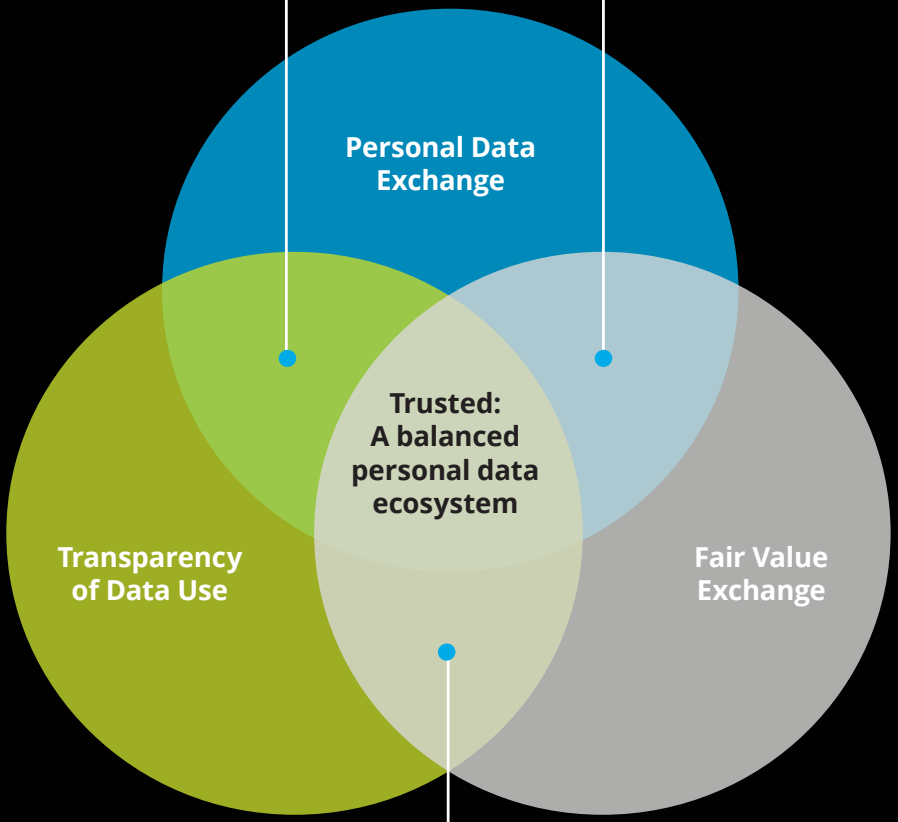
Finding the right privacy balance through transparency and fair exchange of value

DATA EXCHANGE + TRANSPARENCY FAIR VALUE LACKING

Trust can be hard to gain or easily lost if customers don't see a fair return for their personal data

DATA EXCHANGE + FAIR VALUE TRANSPARENCY LACKING

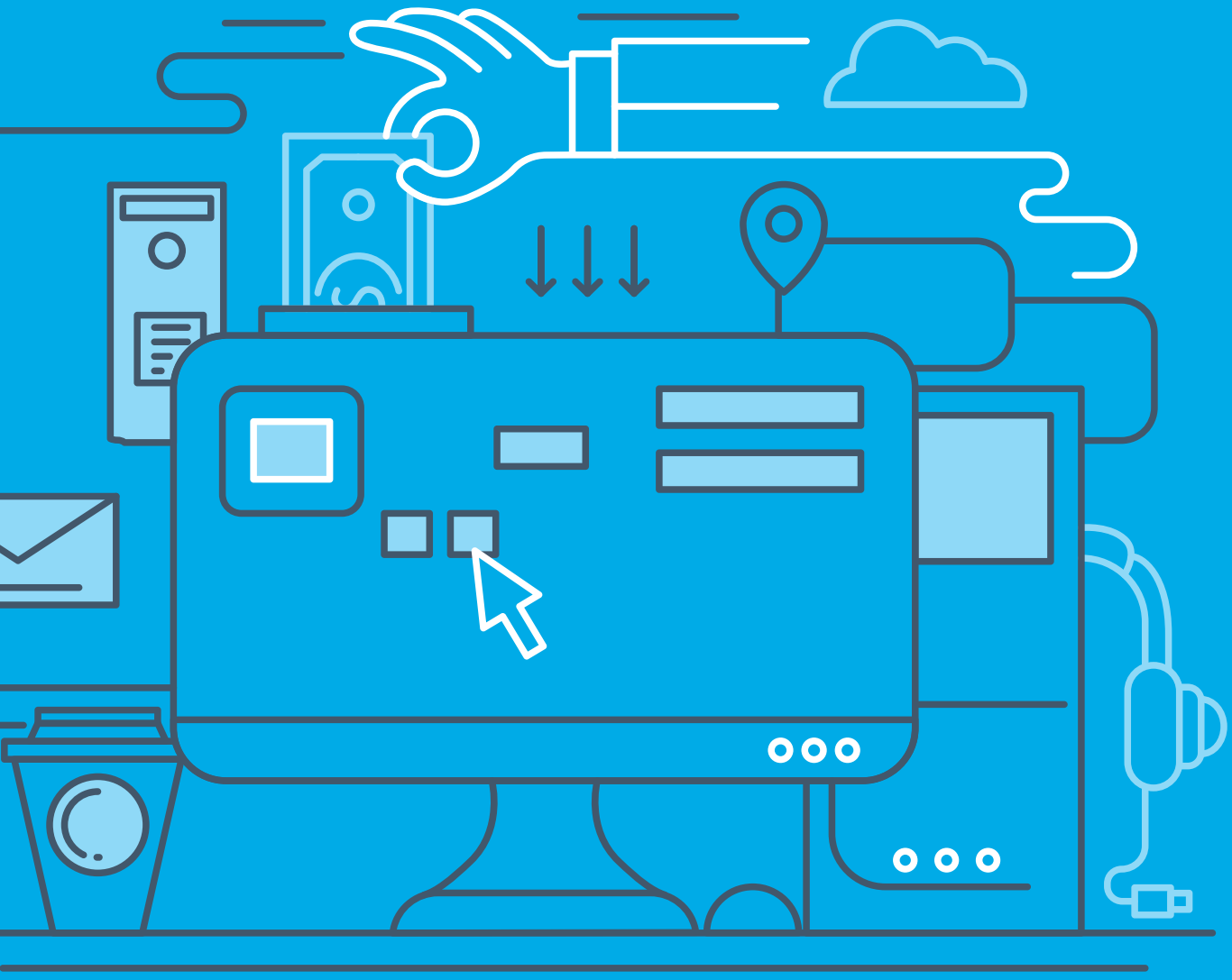
Trust can be hard to gain or easily lost when unexpected and unwanted uses for personal data become known



TRANSPARENCY + FAIR VALUE DATA EXCHANGE LACKING

Trust may exist but lack of personal data may impact the customer experience, in turn making it harder to build a good reputation and trust

Consumer sentiment analysis



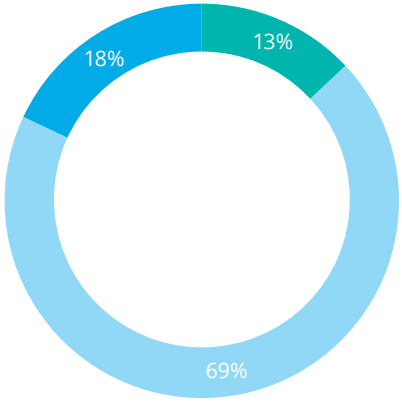
Key insights

The following insights have been developed from the survey results of over 1000 consumers aged 18 and above across Australia.

Considerations that impact the value exchange

Consumers indicated the most important consideration in their decision to share personal information with a brand is the reputation of the brand, with 69% choosing to share information where they trust that the brand will use their personal information responsibly.

What is the most important consideration in deciding to share personal information?



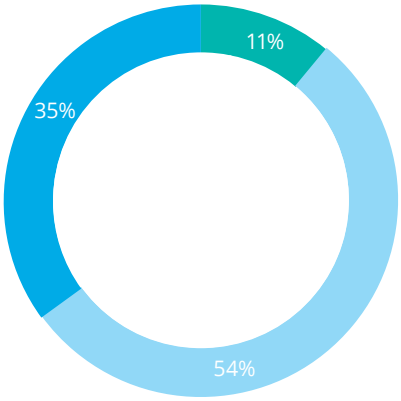
- Products/services customized based on data shared
- Trust that a brand will use data appropriately
- Tangible benefits

The majority of consumers (65%) are unlikely to share sensitive personal information (such as income, health information) with a brand in return for a benefit, for example, to earn loyalty points or to receive a gift.

Consumers surveyed also demonstrated a strong awareness of how personal information is defined, particularly that it can include information such as IP addresses, internet browsing history and cookies. The survey revealed that 60% of consumers in the age bracket of 18-34 have taken active measures not to expose their digital identity (where possible) and have used a pseudonym when transacting online. 76% of consumers indicated protection of privacy was the main reason for masking their true identity.

On views regarding the growing use of smart devices (e.g. connected cars, wearable devices, smart television, home assistants) and the level of personal information that is being collected by brands, 48% of consumers were unsure what the brand will do with that personal information or the practices they follow to protect such personal information.

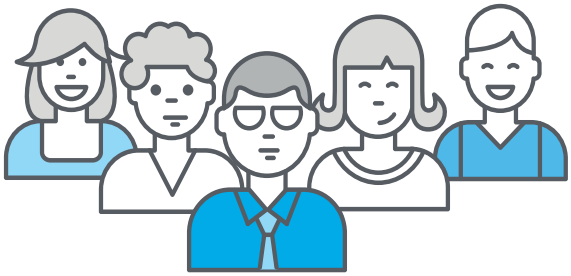
Do you trust smart devices to maintain your privacy?



- Actively use and trust
- Unsure
- Apprehensive

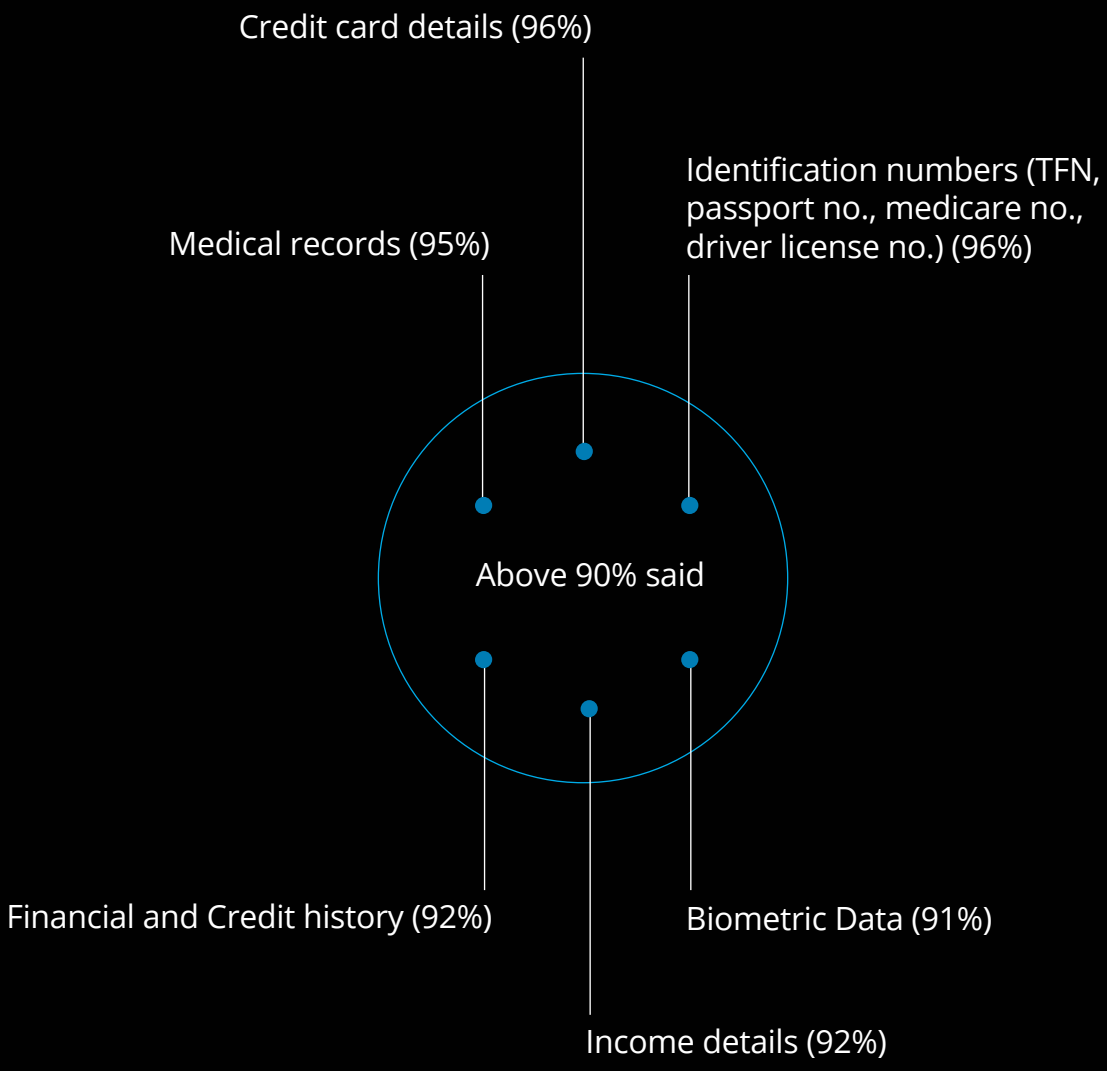
Consumer trust behaviour

Consumers react positively to transparency. Brands that have made a commitment to be more transparent about their personal information handling practices can expect a trust dividend from consumers with 44% indicating that good privacy practices are important for a brand to build trust of its consumers.



Consumer trust behaviour

When asked what they consider personal information to be



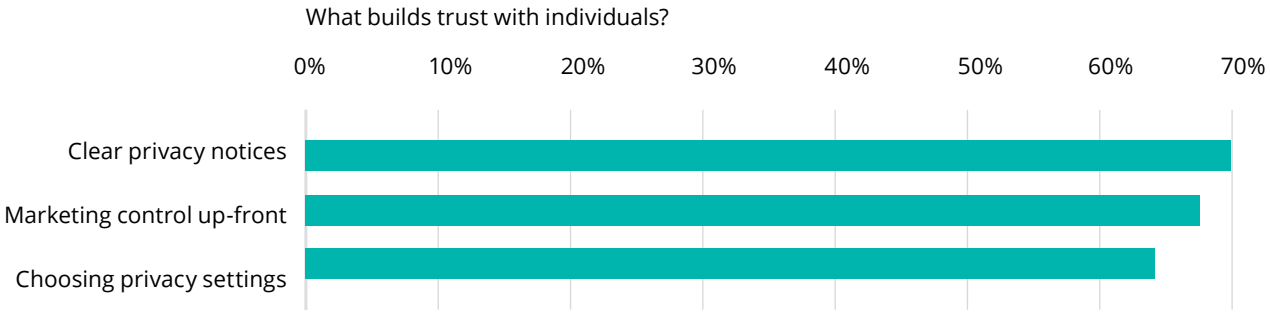
Internet browsing history (78%)

IP addresses and mobile device IDs (78%)

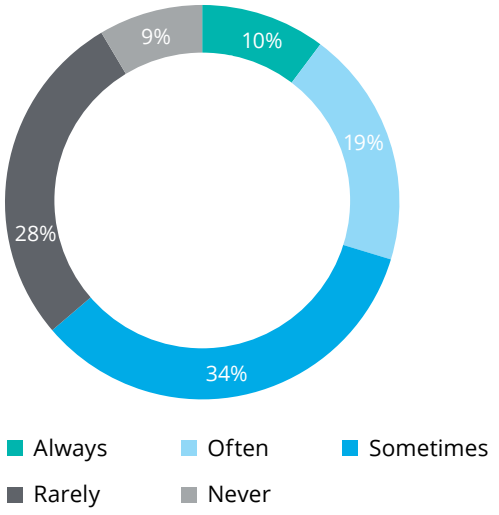
Data collected by browser cookies (60%)

Building Trust

Consumers highlighted that clear, transparent communications regarding personal information handling practices builds trust. Of note, 70% of consumers suggested that they have greater trust in brands with transparent and clear privacy notices.



How often do consumers read T&Cs or Privacy Policies?

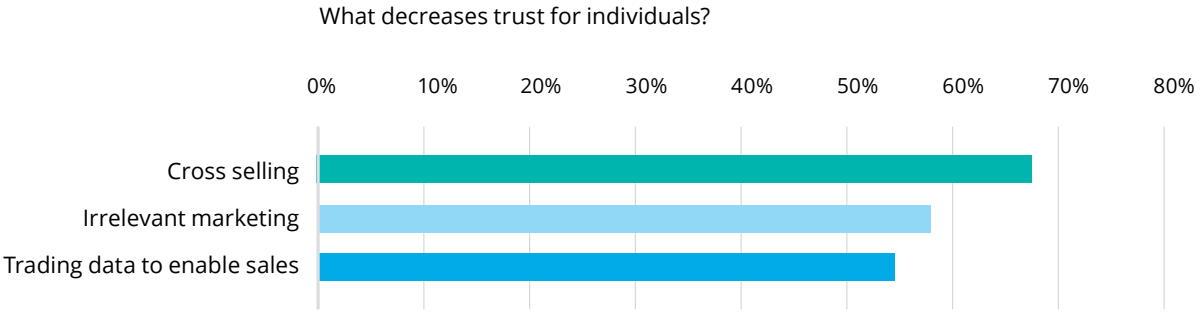


Consumers highlighted that clear, transparent communications regarding personal information handling practices builds trust.

Often terms and conditions are complex, heavily reliant on legal language and must be agreed to, before signing up for a product or service. This statistic highlights the increasing need for documentation free of complex legal terminology and movement toward simple, easily digestible information.

Losing trust

The data from the surveys is clear: customers lose trust in brands when their personal information is used in ways they have not consented to, such as unexpected secondary purposes. The survey responses also reveal that consumers are likely to lose trust in the brands which use their personal information for irrelevant marketing (58%), cross selling (54%) and trading data (68%).



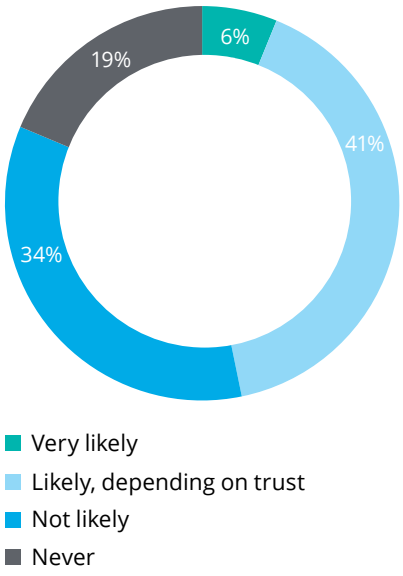
Personal information sharing with third parties

Where personal information is shared with third parties, how you manage that third party is key to maintaining trust.

While most consumers display awareness that their personal information will be shared with third parties, the survey suggests that 53% of consumers are willing to share personal information as long as it is not shared without prior notification or consent.

Concurrently, 41% of consumers indicated that they are comfortable allowing a trusted brand to transfer their personal information to third parties for clear benefits.

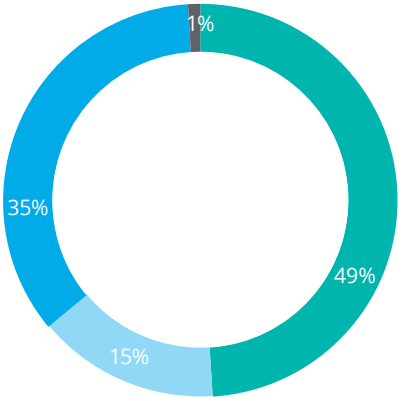
Would you allow a company to trade your data for a benefit?



Regaining trust

February 2018 saw the introduction of mandatory data breach notification requirements in Australian law. The survey data shows that only 58% of consumers are aware of these new mandatory data breach notification laws. Nonetheless 90% expect to be notified in the event of a data breach involving their financial information, health records, family members, home address, mobile number and e-mail address. In the event of a data breach 49% of consumers believe that for their retention as a customer, the brand must provide assurance that it is able to handle the breach.

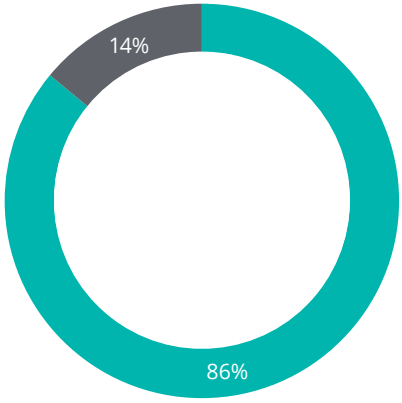
Will you remain a customer of a brand after a data breach?



- Depends on other factors
- No
- Other factors (ease of switching, information involved)
- Yes

The consumer survey indicates that the way a brand responds to data breaches can assist with maintaining a trusted relationship with its consumers. In fact, 86% of consumers indicated that trust may increase in case of timely notification.

Does timely notification increase trust in a brand after a breach?



- Yes
- No

The Symbiotic Relationship: How consumers feel about sharing their personal information for a more tailored and personalised experience?

I wouldn't mind doing this. It would depend on whether I trusted the organisation, what information they wanted, why they wanted it and whether it would benefit me

I want reassurance that my details are not shared without my consent

I'm only willing to share information that's specifically relevant

I don't mind

As long as I feel it will be secure and I can maintain control of the information

I'm happy to share as long as it's not passed on

Don't mind sharing for a reward

I have to trust the brand before I share my personal info with them

I find this helpful if I am being told about products and events relevant to me

I am fine with it if the process is transparent

That depends upon the trust I have in that brand

Only if I agreed. I need to be given the option to say no

Industry insight

A seat at the Chef's table

By Marta Ganko – Executive Manager, Privacy, Westpac Group

If your organisation was a restaurant, where are your customers? Are they in the kitchen, helping you cook, the dining room, or perhaps outside peering in?

On any particular day, a restaurant customer may want to choose what they eat, and not be told what they think the Chef thinks they would like to eat, based on past meal choices.

Similarly in organisations, customers are now asking for more choice about how their information is used, as customer awareness grows. There is an important balance between providing that choice and ensuring the choices provided complement customer awareness.

Striking the balance in this paradox of choice* is a challenge for organisations. Providing little choice can cause customers to seek another service provider elsewhere that better meets their expectations. While equally, too much choice can overwhelm a customer, causing them to seek comfort in a service more easily accessible.

It is crucial that organisations build trust with their customers by getting the balance right. This involves understanding customers' needs and providing requisite transparency, to create a relationship that is of mutual benefit to both the customer and the organisation.

When customers trust that an organisation is willing to invest in their relationship and get to know their individual circumstances, customers become not just another diner in the restaurant, but can instead take a seat at the Chef's table.

* Schwartz, Barry: 'The Paradox of Choice – Why More is Less', Harper Perennial, New York, 2004

Practitioner's insight

The intersection between law, technology and ethics

By Anna Johnston - Director, Salinger Privacy

As we enter a year of celebrating the 30th anniversary of the Australian Privacy Act, I have been reflecting on the attitudinal changes I've noticed since I first started working as a privacy officer, in the late 1990s. Having also been a privacy regulator and specialist privacy consultant, I feel like I've seen every attitude across the spectrum: from resistance to the privacy message, through grudging compliance, into acceptance and now increasingly an embrace of privacy protection as an enabler of business.

Though there is still a long way to go, I see greater awareness of the privacy risks of sharing personal information without due consideration. Following a set of statutory privacy principles is obviously a good place to start, but sometimes mere compliance is not enough. Even technology companies are now talking about the link between ethical decision-making and customer trust.

From my government clients in particular, I see a deeper understanding of the link between protecting privacy in order to gain citizens' trust, and the success of the project. Trust is important not just to avoid a public backlash, but to facilitate either collecting quality data, or best realising the value of the data they hold. They get it: they need community acceptance, or 'social licence', even more than they need legal compliance.

I see privacy management as shifting from legal tick-box compliance to a more nuanced task of finding the appropriate point of intersection between law, technology and ethics. That point is the sweet spot where your customers – be they your citizens, consumers, members, students or patients – will trust both your organisation, and your plans to collect and use their personal data.

Future trends

Future proofing with the advent of new technologies

The trade-off between convenience and privacy

New technologies create new risks. In the past 12 months, there has been an increased offering in artificial intelligence, the Internet of things, analytics and other technologies that aim to make our lives more comfortable and convenient, but often at a price. These technologies are not exclusive to the commercial world but have transcended into our homes and daily lives. While, smart, connected objects offer tremendous opportunities for value creation and capture, they can also create tremendous risk, demanding new strategies for value protection. A single vulnerable device can leave an entire ecosystem open to attack, with potential disruptions ranging from individual privacy breaches to massive breakdowns of public systems.

Points for consideration

- Check out cashiers may soon be made redundant. Instead surveillance and sensors that monitors each consumer entering, shopping and exiting the supermarket automatically deducts from your bank account should you decide you want something off the shelf.
- Internet of Things (IoT) devices fitted at the work place and at home allowing us to be connected 24/7.
- Self-driving cars programmed to suit the driver's needs and able to communicate with other cars. Not only this, but the ability for cars to be directed remotely, or otherwise 'hacked', may have significant detrimental consequences for the passengers.

Brands need to align with newer technological trends and expectations of consumers

1. Go back to basics

Ensure the basics are addressed and implemented by adopting solid design principles such as privacy by design and privacy by default.

Small changes to everyday business processes may result in a high gain to the brand, but understanding and addressing potential privacy implications attached to those changes will help distinguish brands from its competitors. Implementing strong design principles that respects and understand privacy will allow brands to gain the trust from its consumers and thus do more with the data.

2. Keep up with legislative changes

The introduction of the European Union E-privacy Regulation is turning heads. It will bring the E-privacy Directive in line with advancements in technology and harmonise laws across Europe.

Currently, the draft E-privacy Regulation will align to new data protection laws that have been introduced and enacted, such as the EU GDPR. This Regulation will regulate machine-to-machine transmissions such as cookies, telecommunications, and data flows between IoT devices. This regulation is still in draft form and is expected to be finalised in 2018.

3. Profiling, analytics and consent

Profiling and analytics are core to businesses. To stand out from competitors, brands will benefit from being transparent about its processes and obtain consent from consumers to the use of their data.

Expect and welcome change

As consumers become increasingly aware of benefits and risks around the handling of their personal information, evolving public sentiment towards privacy is driving both regulatory and social changes, with a profound impact on brands across all sectors. The EU GDPR, driven by a significant societal shift in regards to data ownership and transparency, is one of many significant changes occurring in this sphere, both abroad and in Australia.

Locally, the Notifiable Data Breach Scheme has now come into effect, requiring the mandatory reporting of certain data breaches by both public and private bodies. Brands should consider that public demand and increasing consumer awareness are likely to continue shaping the regulatory landscape, and further regulation is likely to be forthcoming on matters of public interest or scrutiny.

Rather than attempt minimum compliance, brands should invest in a holistic, dynamic and transparent privacy model and practices. Ultimately, current and future regulatory changes provide brands with an opportunity to enhance consumer trust and confidence, and build a stronger relationship between consumer and brands.

Possible future regulatory changes

- Stricter notification and consent requirements
- More widespread regulation (including that of currently unregulated bodies)
- Additional restrictions in relation to data analytics and marketing
- Additional consumer rights.

Consider your third parties

Recent news has confirmed that brands are missing their opportunity to foster trust in the digital economy by protecting consumers' information. News about digital businesses sharing their consumers' personal information with third parties for purposes unknown to the consumers raise concerns about brands' data practices. But, what should brands do? How can brands leverage their privacy practices to have an additional competitive advantage in the market? These are simple steps that brands should follow:

Help their consumers to understand what data they are sharing

Brands need to be upfront and clear regarding what information will be collected and handled.

Think of a consumer that orders food using a voice recognition device. What information is that consumer really sharing? Certainly not only food preferences and voice characteristics.

That consumer is also sharing information including payment and billing information, geographical location, transcripts of their conversations with the device, interaction history and specifics about their hardware and software settings. Potentially, that consumer may also be sharing health information if the order specifies certain dietary requirements.

Don't get caught out

- Be Ethical – Understand the willingness of consumers to share information to third parties and why.
- Have Capability – Understand how technologies are mining data from APIs and enhance your capability to detect, prevent and control the information.
- Get Aligned – Constantly align your practices to consumer expectations which are dynamic in the world of newer technologies, open data and changing regulations which provide additional rights to the consumer.

Develop well-defined privacy policies and procedures that provide clear information and empower consumers

These are two sides of the same coin. On the one hand, brands should explain in plain English to consumers how they are collecting and handling their information as well as with whom they are sharing it and why. On the other hand, the policies should provide expedited avenues for consumers to exercise their rights and gain effective control over their information. This means that consumers should be able to opt out from brands' data practices as well as effectively require brands to modify, update and delete their information.

Implement a data protection roadmap and strengthen third party due diligence

Brands should identify their weaknesses and develop a flexible roadmap to deliver the desired business outcomes while enhancing consumers' privacy. Special attention should be given to third party providers that may have access to consumers' data. Brands must understand in detail what third parties do and how critical is it that they handle the information in the first place. A way to mitigate these risks is by establishing clear and strict guidelines for the handling of consumers' information.

The privacy landscape for brands is changing at a steady speed. New game-changer regulations are coming into place in 2018, while regulatory and public scrutiny over data handling practices increases.

Brands should not only see data privacy as a compliance exercise. Rather, they should use it as a competitive advantage to leverage their success in the digital economy.

What's your relationship with your consumers?

Do they trust you with their personal information?

There is a need for brands to work with consumers to find a balance between their processing of personal information and privacy obligations. As the competitive advantages of being custodian of large volumes of personal information become more apparent, brands will look to greater collection and creation of personal information to extract more value. At the same time, increasing transparency and awareness of personal information processing activities may lead consumers to be more conservative about what information they disclose to brands. How your brand balances its practices, transparency and demonstrate a fair value exchange for personal information will be key for it to be trusted enough for consumers to hand over the large volumes of data that will be needed for future profitability. So, how confidently can you say that you are a trusted brand from a privacy perspective?

Step 1: For each indicator below, circle the number that indicates how confident you are that your brand effectively performs these activities. For no confidence, select 1. For high confidence, select 5.

Indicator	Confidence scale				
We provide consumers with clear privacy notices prior to collecting their personal information.	1	2	3	4	5
We give consumers the ability to choose what we can and cannot do with their personal information.	1	2	3	4	5
We could tell any consumer how we handle their information, and comply with any requests to correct, erase or port their information.	1	2	3	4	5
We collect and store only the information that we need and we know when it is collected, stored and used.	1	2	3	4	5
All staff members are required to participate in privacy training on a regular basis.	1	2	3	4	5
All staff members are aware of and adhere to all policies, processes and procedures.	1	2	3	4	5
We monitor new regulations or standards and assess our risk exposure.	1	2	3	4	5
We adequately monitor misuse of information by our staff members, third parties and contractors.	1	2	3	4	5
We monitor unauthorised access to information by internal and external parties.	1	2	3	4	5
We report metrics regarding privacy risk to our Board.	1	2	3	4	5
We have well developed data breach management policies, procedures and tools.	1	2	3	4	5

Step 2: Add up all the numbers circled to determine your overall score and next steps.

45 – 55	You have all the right qualities to be a trusted brand from a privacy perspective. You have a good story to tell your customers. Do you believe that your good privacy practices are being rewarded with consumer trust?
35 – 44	You have done well, however there is still likely more to be done to gain trust from a privacy perspective. It is recommended that you conduct a privacy review to look for ways in which you can continue strengthening trust relationship with consumers.
Below 35	You may well be handling personal information responsibly and in line with your customers' expectations, but you may not! Trust is such a valuable brand quality that you should conduct a privacy review to determine where you could be going wrong before it is too late!

Methodology

The Deloitte Australian Privacy Index 2018 was developed from analyses of Australia's leading consumer brands. This annual report measures the state of privacy across 10 brand sectors.

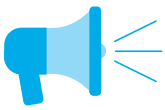
The findings of the Index have been developed from:

1. Survey responses from over 1000 Australian consumers
2. Survey responses from privacy personnel at participating Australian consumer brands
3. Analysis of the publicly available privacy statements of 100 leading consumer brands active in the Australian market.

Consumer survey

An external organisation, Roy Morgan Research was engaged to survey 1000+ Australian consumers to share their understanding of privacy and gain insight to their perception of privacy practices followed up by the brands. A particular focus was put on the perceived relationship between consumers, brands and their use of personal information.

Brand survey



Privacy professionals from leading Australian brands were invited to complete this survey on behalf of their organisation providing a sector side view of privacy today. The brand survey also asked relevant brands about their preparation for global regulatory changes, notably the notifiable data breach requirements effective from 22 February 2018 and the EU General Data Protection Regulation as its enforcement deadline of 25 May 2018 approaches. Some of these key insights are included in the executive summary.

Brand publicly disclosed privacy practice analysis

Analysis was performed on the publicly available privacy statements of 100 brands active in the Australian market. This analysis focused on certain qualitative and quantitative elements of those statements and was assessed by a team of privacy subject matters experts within Deloitte.

References

Law and Regulation

National

- Privacy Act 1988 (Cth)

International

- General Data Protection Regulation 2016/679 (EU)

Regulatory Guidelines and Reports

- OAIC Guide to developing an APP privacy policy, May 2014
- Office of the Australian Information Commissioner, 'Notifiable Data Breaches Quarterly Statistics Report January 2018 – March 2018'

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

- Brand Finance "Global 500 2018: The annual report on the world's most valuable brands", February 2018
- ASX 200

Other references

- Pilgrim, Timothy, Australian Privacy Commissioner: 'Commencement of the Notifiable Data Breaches scheme' (Speech delivered to the Optus Information Security event, Sydney, 22 February 2018)
- Schwartz, Barry: 'The Paradox of Choice – Why More is Less', Harper Perennial, New York, 2004

About the series

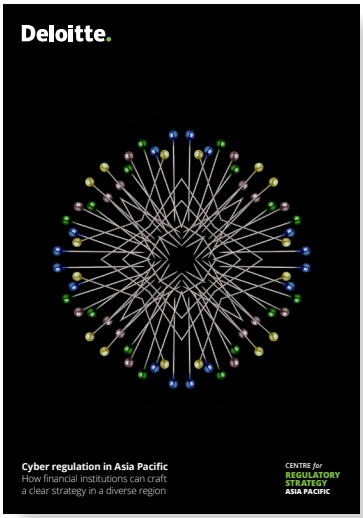
The Deloitte Australian Privacy Index is an annual research report that examines key privacy issues of its time through surveys of customers, surveys of brand representatives and analysis of publicly available materials from top brands indicating privacy practices. Through this research brands are grouped by sectors and ranked on a number of key privacy metrics. Please see the methodology section of this report for more details.

Transparency is opportunity (2015)

Trust without borders (2016)

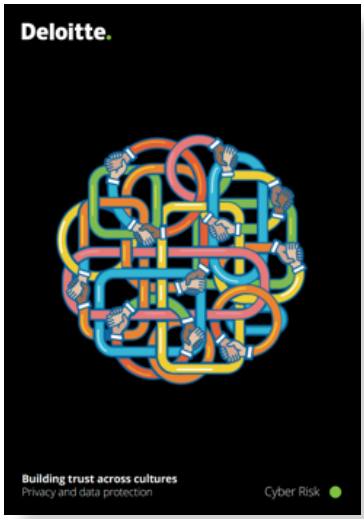
Trust starts from within (2017)

Other publications you may be interested in:



Cyber regulation in Asia Pacific

Voice of Asia



Building trust across cultures

Contacts

David Batch
National Privacy and Data Protection Lead, Risk Advisory, Sydney
+61 2 8260 4122
dbatch@deloitte.com.au

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

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

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

David Owen
Partner, Risk Advisory
Sydney
+61 2 8260 4596
dowen@deloitte.com.au

Katherine Milesi
Partner, Consulting
Melbourne
+61 3 9671 7766
kmilesi@deloitte.com.au

Melissa Ferrer
Partner, Consulting
Sydney
+61 2 9322 7844
meferrer@deloitte.com.au

Deloitte.

MCBD_HYD_04/18_054325