



Trust: Is there an app for that?

Deloitte Australian Privacy Index 2019



“If you want to build trust then really, today, it is about your social licence and making sure your business is not too far away from what society expects. Otherwise, basically, you won’t have a business, because you won’t have customers, you won’t have employees, and you probably won’t have investors.”

Greg Medcraft, immediate past chair, Australian Securities Investment Commission (ASIC), now director of the Directorate of Financial & Enterprise Affairs, Organisation for Economic Co-operation and Development (OECD) Paris AFR, 12 April 2019.

Contents

App-ropriate protection

There are few things more powerful when it comes to building trust than getting your privacy settings right. As community expectations set the parameters of social licence and trustworthiness, 'what you are doing with my data', and 'protecting my privacy' are key.

Hence asking: 'Trust – Is there an App for that?'

In this year's Privacy Index Deloitte examines the privacy characteristics of the mobile apps of the top 100 brands in Australia, what consumers expect and how they interact with their applications. We rank the brands by sector, breaking down our key findings to highlight where brands might be lacking in their app's privacy attributes, and what consumers expect, think and do about their privacy when using the app.

Our inside cover quote from key Australian, and now international corporate governance regulator, Greg Medcraft, encapsulates the danger of not responding correctly to meet such community expectations.

Medcraft believes many companies have been too slow to realise the importance of social licence reference. He is recalibrating the OECD Principles of Corporate Governance to embed a social licence to operate in them, specifying the duties and responsibilities, as well as the rights, of the corporation. Nevertheless, Medcraft is optimistic that the power of social media is empowering those who can drive real change.

This is good news for business and the community.

Knowing an individual's privacy expectations, as well as the corporation's duties and responsibilities, can help ensure that privacy is not unknowingly or disproportionately traded, when using an app. Users expect apps to be easy to use, secure, and personal — not peppered with information or features they don't want. This means they need to share significant amounts of personal information with the app. How to balance these needs is the substance of our 2019 Privacy Index research.

Apps matter for employees

Our findings and recommendations are equally valid for workplace app developers. The Deloitte 2016 Privacy Index suggested that workplace app developers are subject to even greater privacy expectations from employees than customers or clients. In this era of the tech-savvy, app-using millennial workforce, the takeaways from this year's consumer research are just as valid for the enterprise app owner and developer.

Following your followers, understanding them and respecting privacy boundaries is critical. We trust our research will help you build better apps to support your business and customer privacy expectations.



David Batch
National Privacy and
Data Protection Lead,
Risk Advisory



Tommy Viljoen
National Lead Partner
Cyber Strategy and Governance
Risk Advisory

App-bout this report

Consumer sentiment analysis

In this 2019 Deloitte Australian Privacy Index we surveyed more than 1000 Australian consumers aged 18 and above asking them about their personal privacy practices when interacting with their mobile apps. We asked:

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

We also asked how they feel about privacy in the mobile app environment and its impact, asking:

- How privacy impacted their behaviour and views followed the app engagement 'lifecycle'
- How privacy impacted their decision to download an app
- How they used an app
- If privacy concerns led to disengagement or deletion of an app.

Brand analysis

Here we investigated the publically available privacy policies of Australia's top 100 consumer brands that have a consumer facing mobile app.

Our team of researchers examined the privacy behaviours and attributes of those apps, focusing on the features that gave consumers the ability to control their personal information.

The Index

This year we analysed brands by assessing the privacy practices of their branded mobile apps. We only compared the brand apps running on the iOS environment because of the uniformity of privacy requirements given that the single origin app store and our consumer research shows almost half (46.6%) of survey respondents use an Apple iPhone, making it the most used brand handset in the Australian market.

We combined the findings of the brand analysis with selected findings from the consumer survey, as well as sector level breach and complaints data published by the Office of the Australian Information Commissioner (OAIC).

The results were scored and aggregated across 10 industry types enabling us to rank each of rank each industry to create the Index.

Results

All responses to surveys are confidential and anonymised. The Index and accompanying report aggregate responses that that are statistically analysed to provide insights into key privacy practices and perceptions of mobile applications and how each industry is perceived more broadly by consumers.

Acknowledgements

We would like to acknowledge the following for their support:

- Roy Morgan Research Ltd for conducting the consumer survey on behalf of Deloitte

App-etite for control – Key insights

This year’s Index highlights the significant differences in maturity of privacy practices across brands and sectors and a growing consumer awareness of privacy, and their strong desire to take control of their data.

When downloading an app...



Consumers demand **privacy**

65%

of consumers cited trust in a brand as their #1 consideration when deciding to grant an app permission to access personal information. This means brands must be transparent about how they will use personal information.

52%

of consumers have used privacy enhancing applications such as VPNs, browsers with private browsing mode, or encrypted messaging apps to enhance the privacy settings over those available on their handset.

89%

of consumers have at some point denied an app access to their location, photos, and contacts, or features such as their mobile device’s camera or microphone, due to privacy concerns, which reduces the effectiveness of an app to deliver its best product or service.

63%

of consumers deleted apps due to privacy concerns. Consumers will leave brands with apps that do not protect their privacy.

When using an app...

46%

of consumers are likely to provide false personal information when engaging with an app because of privacy, so hindering the accuracy and usefulness of data collected by brands.

59%

of apps allow consumers to partially opt out of the collection of their data, suggesting that brands are beginning to recognise the need to provide consumers with greater transparency and some form of control.

78%

of brand apps provide users with access to a privacy policy or information about their privacy practices within their application.

only 21%

of organisations have indicated that users have the ability to delete, or request their personal information be deleted.

Privacy policies

are not accessible in 22% of apps. Basic transparency requirements of privacy law in Australia are not being fully met.

Technology brands were the most trusted brands for privacy, yet some telecommunications and media sector brands, especially social media brands, were the least trusted.

Top five takeaways for better app privacy



Top five takeaways for better app privacy

1. Give users control

App users need to feel they are in control of how their information is used and why. Use the privacy settings available to developers on key platforms to give granular control to those for whom privacy is very important.

2. Be transparent

Be clear about why you want information that people are sensitive about, such as access to location, cameras, microphones and photo albums. Make it easy for people to keep using your app if they restrict access to such sensitive information, otherwise they are likely to disengage completely.

3. Assess your privacy risk early in design

At the app design stage, conduct a Privacy Impact Assessment to ensure you minimise the privacy risk that your app is exposed to. Minimise the data collected, verify how and when you will use data, and to whom you will disclose it. Also give a clear time limit for how long you retain that data.

4. Follow the OAIC guidelines for mobile developers

At an absolute minimum, build in the requirements of the OAIC's 'Mobile privacy: a better practice guide for mobile app developers' available on OAIC's website.

5. Follow the mobile platform rules for privacy best practice

Whether you are developing on iOS, Android or another mobile platform, ensure you follow all the privacy best practice guidance provided by the platform.

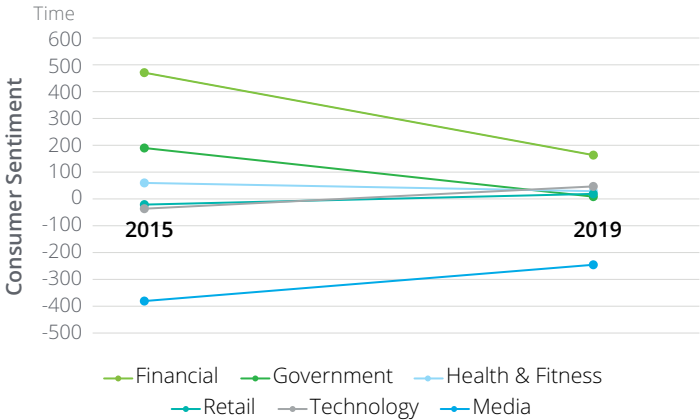


Privacy Index 2019: How each sector ranked

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

By focusing on mobile applications the sector privacy rankings have shifted significantly this year. Information technology retains its first place ranking from 2018 but Financial has dropped from second place in 2018 and first in 2016 and 2017 to ninth, and Government from third in 2018 to eighth this year.

Trust in privacy five years on



Each year we ask 1000 consumers which brands they trust the most and which they trust the least with their privacy. Those results are then aggregated across industry sectors, returning a net negative or positive trust in privacy score.

From our first Index in 2015 to now, there has been some significant movement in the consumer trust in privacy scores. Financial services has seen the biggest loss in trust in privacy, but is still in positive territory, meaning more consumers trust than distrust financial services brands with their personal information. Government has also had a significant drop in trust in privacy over this period, returning a near zero result in 2019, meaning there were as many consumers saying they trusted as well as distrusted government with their privacy.

Index insights

The most trusted brands

- **31%** of consumers named Information Technology brands in their most trusted brands. The combined results of our Index also rated Information Technology as the top performing sector, which indicates a growing consumer awareness of, and ability to discern, good privacy practice.
- We also found that consumers actively choose to support brands they believe respect privacy:
- **73%** of consumers are customers of the brand they trust the most with their personal information.
- **38%** of those said they were customers of those brands because of their privacy practices.

The least trusted brands

- **49%** of consumers trusted Telecommunications and Media (including social media) brands the least. Social media brands were the most significant contributor to the least trusted Telco and Media sector status. This sector also rated below average in our app research, highlighting the alignment between consumer sentiment and brand practices.
- Some of these brands have such great market share because they effectively monopolise the goods or services in high consumer demand in their sector. In this instance, consumers will still interact with that brand's app regardless of their level of trust in that brand. However, these brands should note that:
 - **38%** of consumers revealed they used the brand apps they trusted the least, but said they would cease using that app if there was a better alternative, specifically due to their poor privacy practices.
- Even with significant market share today, these statistics reinforce the importance of strong privacy practices in a competitive economy, and the importance of privacy to sustain business models.

Other inputs for the index

- **OAIC Notifiable Data Breaches Report**
We used data from the 2018 OAIC quarterly reports on the Notifiable Data Breaches scheme (between January and December 2018). The top consumer sectors reporting breaches were Health, Finance and Education.
- **OAIC Consumer Complaints Report**
We used the most recent complaints data from the OAIC, which is organised on a sector basis and indicates the number of complaints received by members of the public. The top sectors were Finance, Health, Government, Telecommunications, Retail and Utilities.

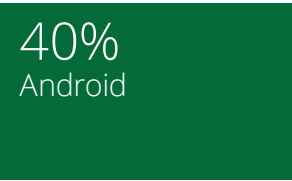
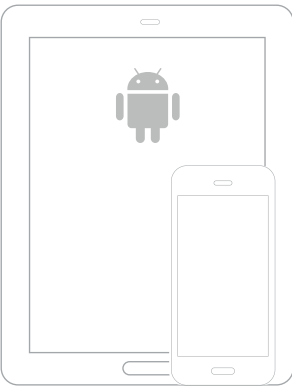
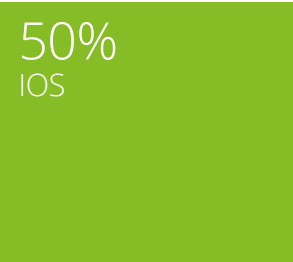
¹ OAIC, Notifiable Data Breaches Quarterly Statistics Reports – January 2018 – March 2018, 1 April – 30 June 2018, 1 July – 30 September 2018, 1 October – 31 December 2018

Consumer sentiment analysis

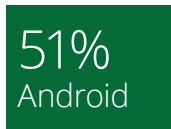
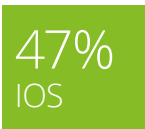
The mobile app market

What does the mobile app market look like in Australia?

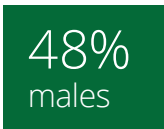
Mobile device OS (incl. tablets)



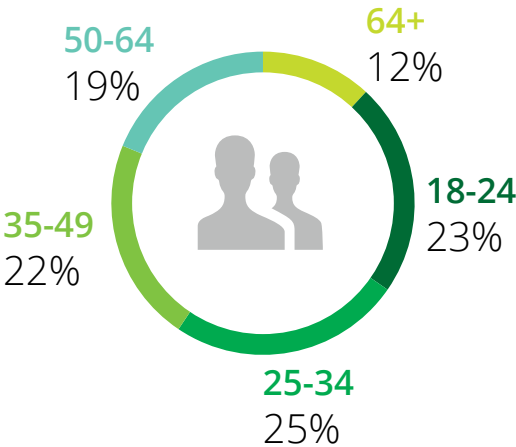
Consumer smartphone operating systems



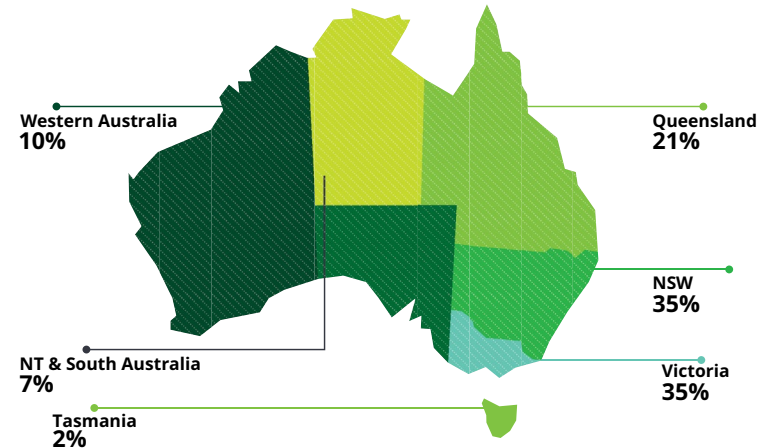
Consumers



Smartphone market by age group



Smartphone market by location





“If you are not paying for it, you’re not the customer; you’re the product being sold.”

Andrew Lewis

Choosing an app

98%

of consumers believe privacy is at least **somewhat important** when deciding to use an app.

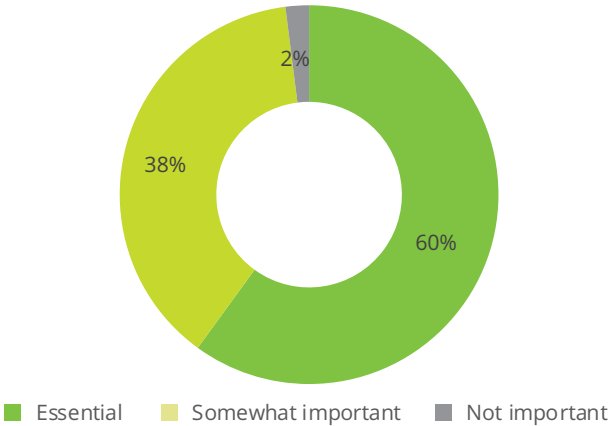
>60%

think privacy is **essential** when choosing a new app.

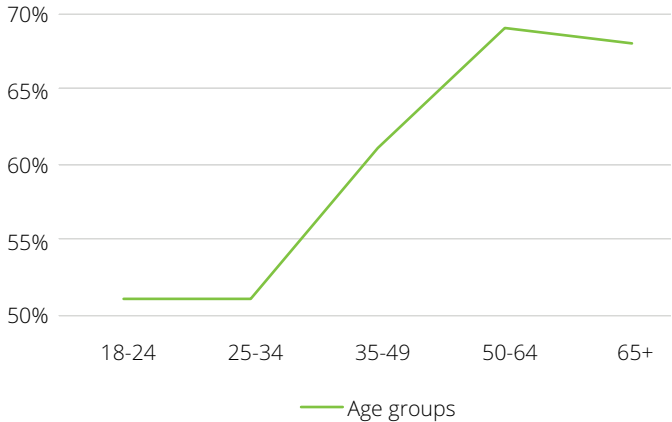
A mere 2%

don't consider privacy at all.

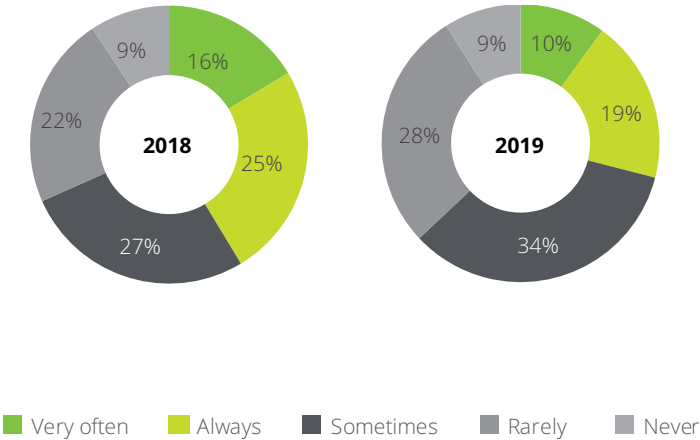
How important is privacy for you when deciding to use a new app?



The importance of privacy to consumers **increases with age**. Older age groups were more likely to state that privacy was an essential consideration when deciding to download a new app.




How often do you read at least part of the app privacy policy before downloading an app?



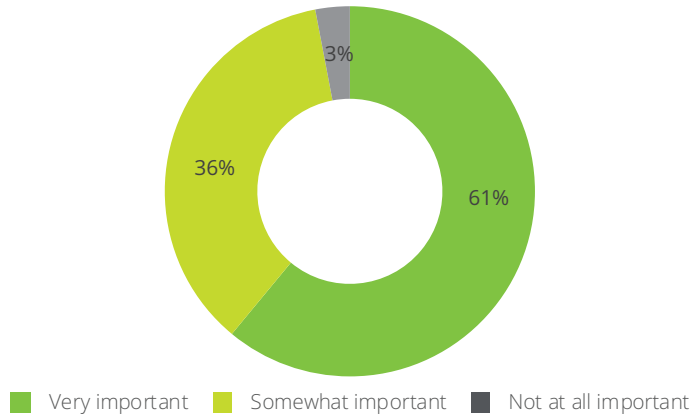
68% of consumers indicated that at some time they have read at least part of a privacy policy before they decided to download a particular app.

12% The percentage of consumers who 'always' or 'very often' read privacy policies grew 12% between 2018 and 2019, highlighting growing awareness and vigilance in consumers, likely due to increased regulatory and media attention to privacy issues.



As a stand out, **81%** of Tasmanians indicated that at some time they have read part of a privacy policy before downloading an app.

How important is it to you that applications have a clear privacy policy?



Interestingly, while the vast majority of people don't read privacy policies every time, the majority have indicated that they have at some time. Reflecting and even exceeding these figures, 97% of Australians believe it is important for a brand to have a clear and transparent notice of how their personal information will be used. This indicates that brands now need to consider, more than ever, how their privacy policy reads to the average consumer and whether it serves its purpose as an understandable source of information and transparency.



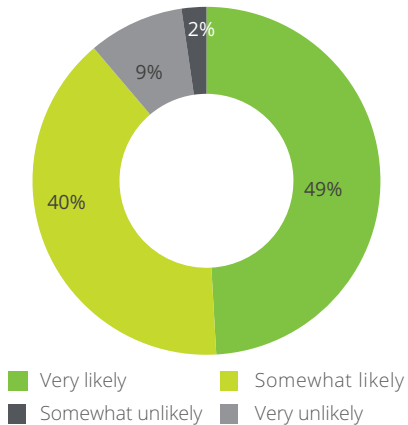
In their hands: managing privacy while using an app

Once downloaded, consumers expect to be able to manage their app's privacy settings, tailor it to their personal needs, and increasingly take control of their own data.

Permissions

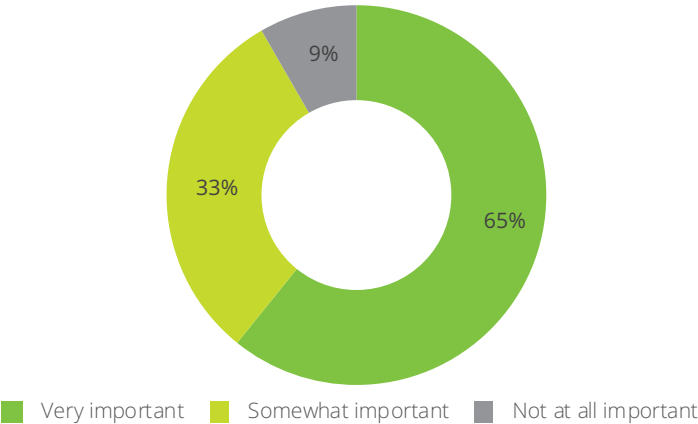
Permission settings allow consumers to grant or deny access and so give them a level of control of their privacy.

When installing or using apps on your Smartphone, how likely are you to deny or decline that app permission to access such as your location information, your pictures, your contacts, your camera or your microphone?



89% of those surveyed indicated that they are either 'very likely' or 'somewhat likely' to deny apps access to certain personal information.

How essential is trust when choosing to grant/deny app permissions?



When considering how they will manage permissions, consumers highlighted trust in a brand as part of their decision to grant or deny access to their information.

65% said trust in a brand was essential when deciding whether to provide access to personal information, or allow permissions. This reflects the importance of reputation, its impact on consumer behaviour and how limiting access to data may effect the performance of an app as a result.

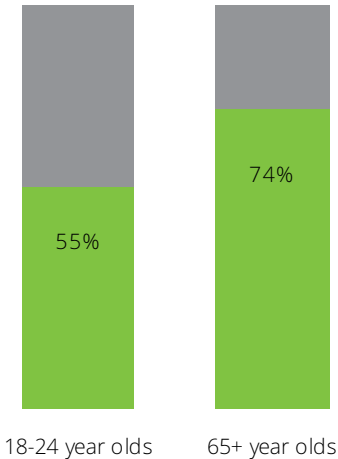
According to the Australian Community Attitude to Privacy Survey 69% of Australians in 2017 were more concerned about privacy than they were in 2012.²

There are also demographic differences when asking consumers about the importance of trust when granting permissions. Those over 65 found it 'most important', with **74%** considering it 'important', opposed to **55%** of 18-24 year olds.

In the 2018 Deloitte Australian Privacy Index, 70% of consumers indicated that clear privacy notices (which includes privacy policies and point of time notifications), build their trust in a brand. 65% thought that allowing for control of marketing up-front built trust. 60% felt that having control over privacy settings increased their trust.

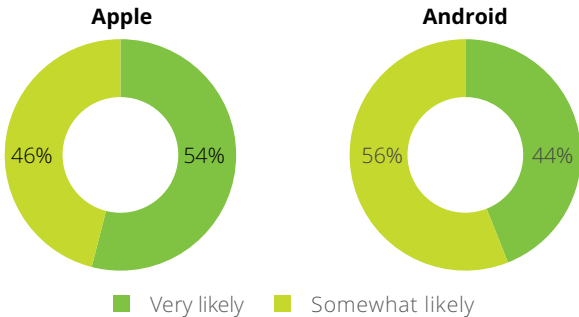
²Australian Community Attitudes to Privacy Survey 2017

How likely are Apple and Android users to deny apps access to permissions?



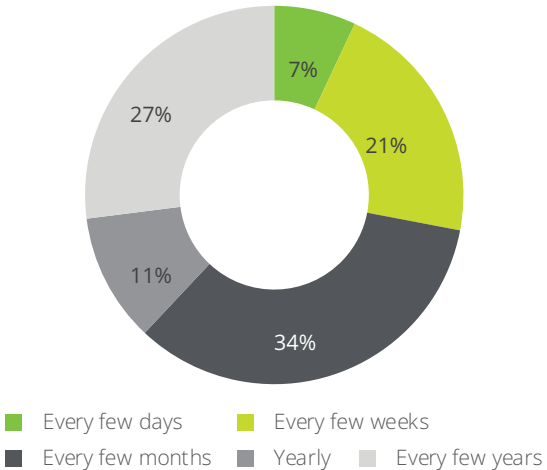
54% of apple users are ‘very likely’ to deny personal information access permissions from apps than Android users (44%).

This continuing management of privacy settings by consumers reflects increased engagement with privacy, and shows it is more than a one-off for most consumers.



How often do you check personal information access permissions for applications regularly used?

34% of consumers checked their permissions every few months, and a healthy 21% checked them weekly.

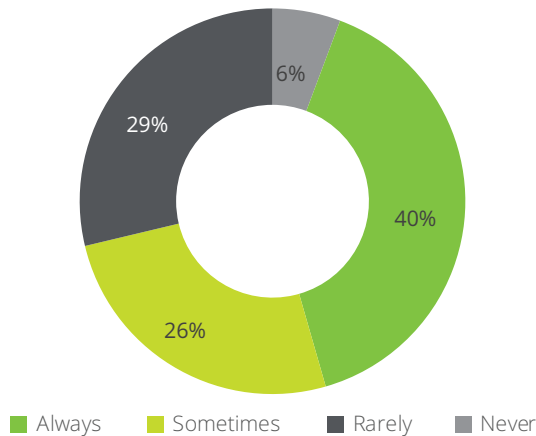


False information

Providing false information can both affect the personalisation experience for the consumer, and the business strategy of an organisation.

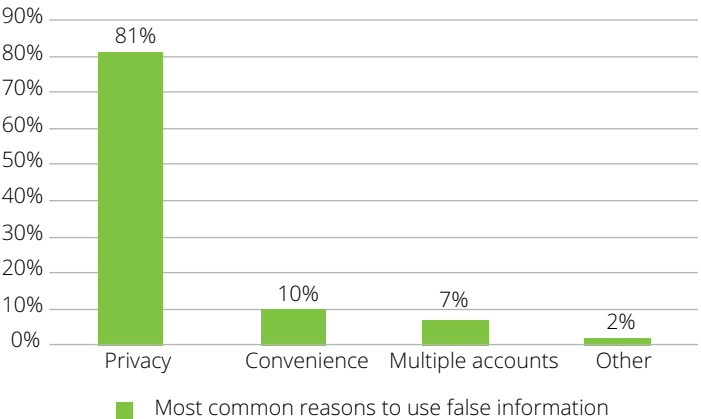
Organisations rely on the accuracy and completeness of consumer data they collect from mobile applications for a variety of tasks, including market research and analytics. False information will impact business goals.

46% of consumers are likely to provide false information through an app if they can.



Organisations must consider the repercussions on their business if a large part of their information is invalid.

What is the most common reason you would use false personal information for your apps?

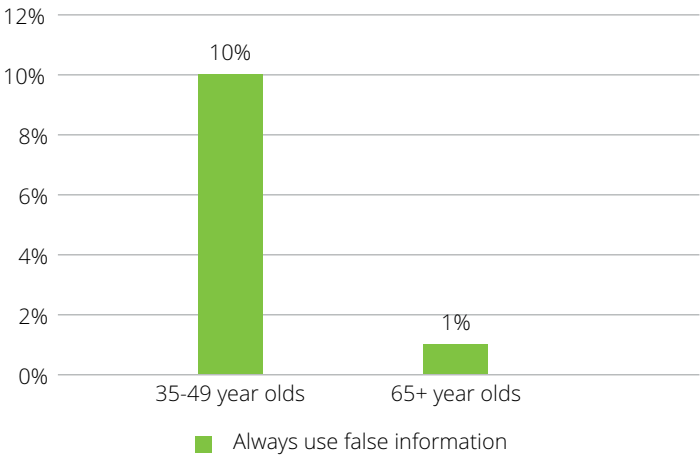


81% of consumers cited privacy as the most common reason for providing false information.

Organisations with issues around false information could strengthen their privacy practices so consumers would reconsider their actions.

How often do you provide false personal information to apps?

10% of 35-49 year olds always use false information. The clear demographic split between who ‘always’ provide false information vs. 1% of 65+ year old.



Enhancing privacy

Consumers may also choose to enhance their privacy by using tools at their disposal such as private browsing, VPNs and encrypted messaging applications, taking control of their own data past the control of the organisation they are patronising.

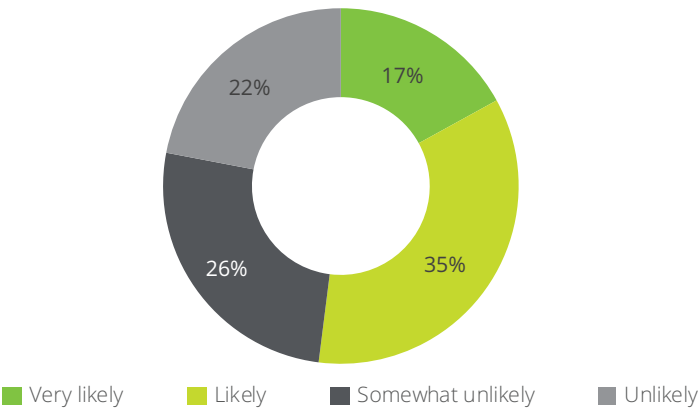
52% of consumers were likely to use privacy enhancing applications, indicating the majority of consumers are aware of and prepared to act on improving their privacy by taking additional steps above settings provided by brand applications.

How likely are you to use privacy enhancing applications?

There was a marked difference in how age groups use privacy enhancing applications.

35-49 year olds were most likely to use privacy enhancing applications. **58%** said it was likely they would use privacy enhancing applications.

36% of 64+ year olds would use privacy enhancing applications. As tech-savvy younger users enter the market, greater use of these technologies is likely.



More than **50%** of consumers consider the following features important to manage their privacy:

- Access control
- Permission control
- Encryption



Are you sure you want to delete this app?

Consumers are willing to take action against brands and delete apps that don't respect their privacy.

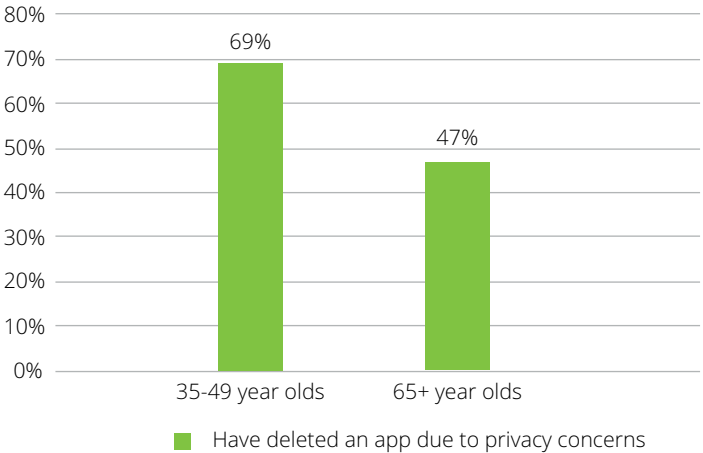
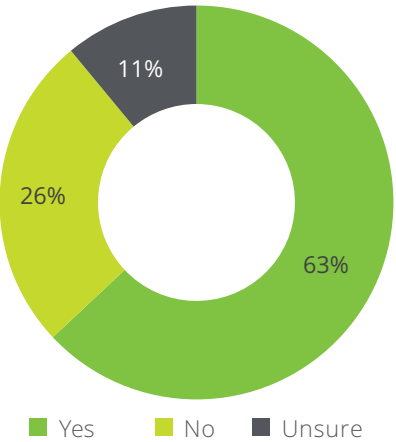
Have you ever deleted an app due to privacy concerns?

63% of Australian consumers have consciously deleted an application as a result of their privacy concerns.

71% of Queenslanders have deleted an app due to privacy concerns, as have

68% of South Australians, 65% of New South Welsh and 64% of Western Australians.

Of those studied, 35-49 year old had most commonly deleted apps previously, contrasting with 47% of 65+ year old.



Respondents who placed greater value on trust correlated positively with those who would delete an app due to privacy concerns.

Consumers more concerned with trust were more likely to take action. 69% of consumers who said trust is 'very important' deleted apps due to privacy concerns. 55% of users who said trust is 'somewhat important' deleted apps, suggesting that less value placed on trust correlates to less immediately related action.

NOTE: A data breach does not mean the end of consumer engagement. According to last year's Deloitte Privacy Index, transparency after a breach can and often does increase the chance that a consumer remains with a brand. 86% of consumers reported their trust in a brand would increase after a breach if timely and transparent notification was given.



Brand analysis

As the scandals of misuse of personal information have hit headlines locally and globally over the past 12 months, FY20 is shaping up to be crunch time for privacy with new privacy laws being considered in many countries.

Flying in the face of social licence

Despite last year's implementation of the European General Data Protection Regulation (GDPR), which attracted unparalleled coverage and attention around a consumer's privacy rights, some organisations continue to obtain, use and retain personal information without the consumer's knowledge and meaningful consent.

To frame our investigation of the mobile app privacy environment and find out how brands can build trust, we researched if they provide control and transparency to consumers and whether they are doing enough to ensure users are informed and aware of how their personal information is being used.

The Office of the Australian Information Commissioner (OAIC) has developed guidelines for developers of mobile applications to ensure a higher standard of privacy protection in their apps. These guidelines outline privacy responsibilities and suggest best practice methods for collection, storage, access, use, and disclosure of personal information.

In our research, to ensure a baselined study, we analysed brand apps from the Apple app store operating on the iOS operating system. We selected this store as iOS holds the majority market share for mobile apps in Australia when considering both smartphones and tablet use. Apps from the iOS store are also subject to a common standard set of minimum development requirements, including those that relate to privacy protection. It should be noted that Android is the most used smartphone operating system. See the Consumer Analysis section for statistics.



³OAIC, Mobile Privacy: a better practice guide for mobile app developers

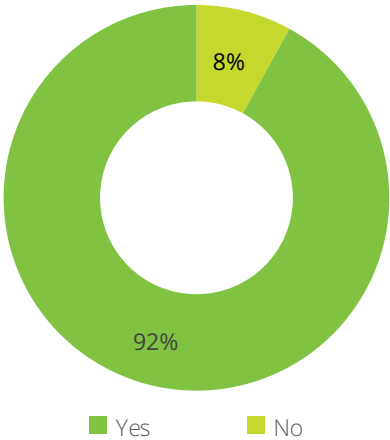
Setting up

The privacy policy

Organisations employ significant resources to ensure the privacy policies created for their applications follow the required legal guidelines. Falling on the wrong side of privacy laws can have drastic ramifications on an organisation's performance and reputation – but how effective are organisations in helping their users find and understand their policies?

Is the privacy policy easy for users and potential users to find?

Is the privacy policy easy for users and potential users to find?



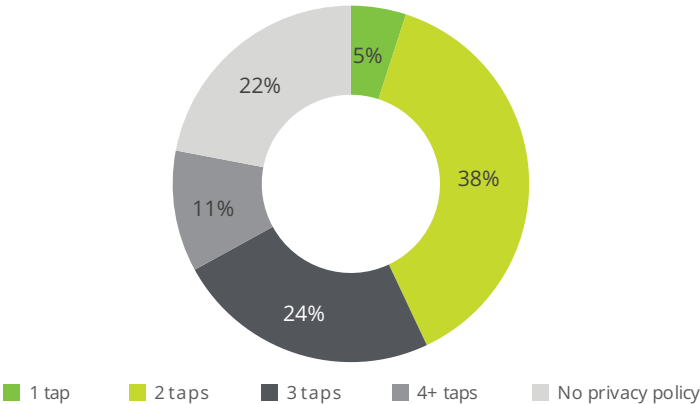
Of the 100 brand apps studied, **78%** provided users with access to a privacy policy within their application. Of those organisations with privacy policies, only **49%** were easy to find (accessible with one or two taps).

The financial sector was the best performing industry, with **94%** of finance apps providing a privacy policy.

The energy and utilities sector also performed well, with **88%** of apps having privacy policies that were also easy to find.

At the low end of the spectrum, **56%** of government applications provided a privacy policy, and in all cases these required 3 or more taps to access.

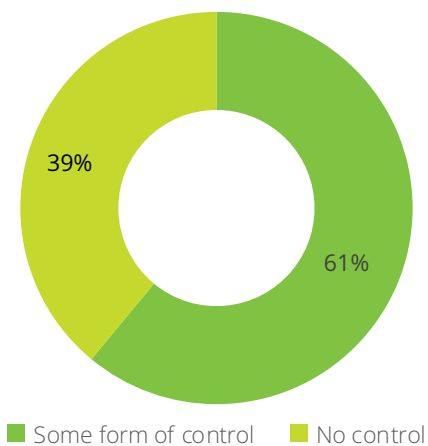
60% of consumers stated privacy is essential to them when deciding to use a new application. The most useful privacy policy for these consumers therefore is one that is both accessible and easy to understand. A policy that is 'simple to understand' is one that states and clearly explains to users what the application is doing with their personal information.



Third parties

Consumers place their personal information in the trust of brands when using their apps, so organisations must ensure they act in accordance with their obligations under privacy laws when it comes to third parties. This includes appropriate privacy controls being implemented that align with customer expectations.

Do controls, such as conditions of contract or user agreements, exist to ensure that third parties respect consumer privacy?



According to their privacy policies, a significant 61% of organisations had controls in place that ensured third parties accessing personal information through an application respected user privacy.

Energy and utilities were the best performing brands, with only one brand failing to indicate the existence of proper controls to protect user information.

Health and fitness also performed well, with 85% indicating that third parties accessing personal information respect the privacy of users.



Passing the power: consumer choice while using apps

Transparency

Prompting consumers to read and accept the privacy policy or other notification on personal information handling on first opening an app is a strong step towards transparency and building trust (see our Consumer Analysis section), empowering the consumer to take control of their personal information.

We examined apps that asked for this type of ‘express consent’ from users to manage their personal information.

15% of organisations obtained express consent from users at first opening of the application after download.

Note: In our analysis, express consent was not obtained if the user accepted general terms and conditions rather than a dedicated personal information handling notice or privacy policy.

What permissions do apps ask for from consumers?

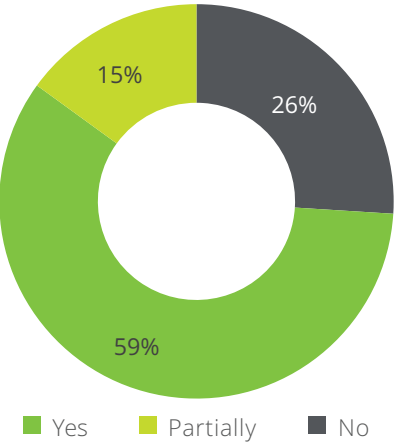
44% of apps asked to use location data at first use. apps also asked to use the consumer’s camera, contacts and microphone.

We found that almost half (49%) of consumers were very likely to deny or decline some or all of these permissions to an app.

Control

Allowing consumers to opt out of the collection of their personal data (or explaining its necessity) is another step that increases trust with consumers, and provides them with the greatest level of control over their personal information.

Can consumers opt out of the collection of their personal information, or is it explained why collection is necessary?



26% of apps allowed users to fully opt out of data collection, or had an express, point-of-time explanation as to why it was necessary for certain functions of the app, so the consumer could make an informed decision on whether to use the app.

If complete opt out is not possible, allowing for partial opt out is a good step. 59% of apps let a consumer partially opt out of the collection of their data for some purposes. The most common options were cookies and marketing e.g. market research and analytics.

Of the 82% of apps that do not ask for express consent when first opened, 28% let their users fully opt out of the collection of their personal information or informed them why this was not possible.

These features give consumers who might be more concerned about their privacy the ability to control their information. They also cater for those who are more likely to seek out and read a privacy policy. However, consumers who don't are restricted from benefiting here.

No industry had more than 50% of their apps offering users the chance to fully opt out of personal information collection. Of the brands studied in the information technology sector, none afforded this opportunity to consumers.

After deletion

Consumers are likely to delete the apps that they download at some point. Our Consumer Analysis discusses what part privacy plays in this.

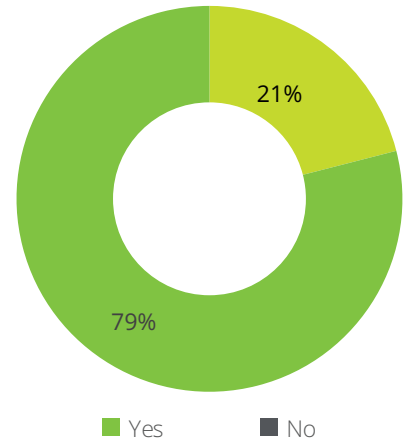
After a consumer has deleted an app, organisations need to consider whether they still require their personal information.

On average, consumers will delete an app approximately six days after they last used it.⁴

⁴eMarketer. (2018). Most apps get deleted within a week of last use.

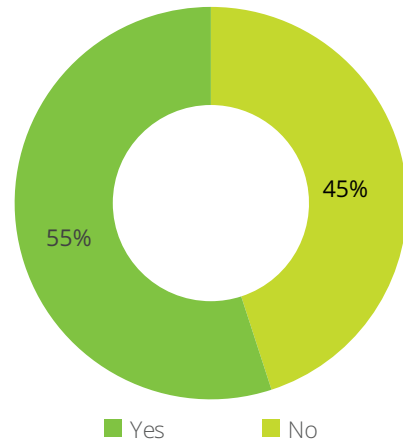
When personal information is no longer required for the purpose for which it was collected, brands must take reasonable action to destroy or de-identify the data.

These practices are encouraged by regulators as they help to build trust between the brand apps and their users, and potentially reduce any impact in case of a breach.



Identifying deletion or anonymising data practices in privacy policies is also a good way for brands to better inform consumers of their privacy practices.

Keeping or deleting data
Is personal information that is no longer needed, deleted or de-identified?



The majority of brands (55%) did not mention deleting or de-identifying information in their privacy policies.

While this may not necessarily indicate that they do not do this, clearly stating what they do in a privacy policy, clearly improves transparency from a consumer standpoint.

Health and fitness and information technology performed well in this area, with 85% and 67% of brands respectively mentioning the deletion or de-identification of personal information that is no longer needed.

Telecommunications and media mentioned this the least frequently, with only 19% of brands indicating they delete or de-identify a user's personal information when no longer required.

Consumer control

Consumers deleting apps might also look to delete (or have deleted) the information a brand has gathered about them. Allowing a consumer to delete information held about them allows a further and final opportunity to control their personal information.

Can consumers delete or request the deletion of all of the data that the app has collected about them?

Only 21% of apps gave notice that the user has the ability to delete or request their data be deleted.

This implies that brands are reluctant to give users the opportunity to remove personal information, sending a potential message that they want the full control over the collected data, rather than the consumer.

In the Information Technology sector 67% of brands had a provision in their privacy notice indicating that a user has the ability to either delete or request their data be deleted, in contrast to all other industries, where the majority did not indicate this.

⁴eMarketer. (2018). Most apps get deleted within a week of last use.

Building trust

Apple: Developer tips for protecting users' privacy

Designing for user privacy is important

Apple devices contain personal data that users don't want exposed to apps or third parties. If your app accesses or uses data inappropriately, the user might stop using your app and even delete it from their device. [Read more](#)

Access user or device data only with the user's informed consent

Take steps to protect any data collected and be transparent about how you use it.

Only request access when your app needs it

For example, a navigation app needs a user's location but does not need their health history or access to the camera.

Provide a purpose

Provide clear usage descriptions when requesting access to user data and account for scenarios when a user does not give permission. [Read more](#)

Give the user control over data

Provide ways to disable access to any data you cache or collect outside of the system protections. For example, if your users build a social media profile containing personal information, offer them a way to delete the data (including any server copies you have).

Protect data you collect

Encrypt your app's files by using iOS's native data protection, which is enabled automatically when a user has a passcode turned on. By default, files are inaccessible until the first time the user unlocks the device. After the first unlocking of the device, the file remains accessible until the device shuts down or reboots. Developers can specify additional data protection levels. [Read more](#)

Most of us use apps in our day to day lives as consumers, and increasingly companies are relying on apps so we can work the way we live. Deloitte and Apple have teamed up to help companies quickly and easily transform the way they work by maximizing the power, ease-of-use and security the iOS platform brings to the workplace through iPhone and iPad.

[Read the press release](#)



Methodology

The Deloitte Australian Privacy Index 2019 analysed the state of privacy of Australia's leading consumer brands across 10 brand sectors.

The findings of the Index were developed from:

1. Survey responses from more than 1000 Australian consumers
2. Analysis of the mobile apps of 100 leading consumer brands active in the Australian market
3. The OAIC Notifiable Breach Scheme Report (1 October to 31 December 2018)
4. OAIC Consumer Complaints Data

Consumer survey

An external organisation, Roy Morgan Research, was engaged to survey more than 1000 Australian consumers to share their opinions of privacy and gain insight into their perceptions of privacy practices followed by various brands. The focus was on how consumers control their privacy when using mobile applications.

Brand analysis

We analysed the branded mobile applications from the top 100 brands in Australia, downloaded from the Apple app store according to a question set developed from the OAIC's mobile application guidelines. Inputs included the application's privacy policy and consumer facing app features. We ascribed higher value (or weight) to the questions that aligned with the consumer perspectives of important privacy features that were informed by our consumer survey, than those purely concerned with features such as clauses in an app's privacy policy.



References

Law and regulation

National

- Privacy Act 1988 (Cth)

International

- General Data Protection Regulation 2016/679 (EU)
- Regulatory Guidelines and Reports
- OAIC, "Mobile privacy: A better practice guide for mobile app developers", September 2014
- OAIC, "Notifiable Data Breaches Quarterly Statistics Report: 1 October – 31 December 2018" December 2018

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

- Brand Finance "Global 500 2019: The annual report on the world's most valuable brands", January 2019
- ASX 200

Other references

- Appfigures, (2018). 'iOS Developers Ship 29% Fewer Apps In 2017, The First Ever Decline – And More Trends to Watch'. Retrieved from <https://blog.appfigures.com/ios-developers-ship-less-apps-for-first-time/>
- Grover, R., & Vriens, M. (2006). The Handbook of Marketing Research: Uses, Misuses, and Future Advances. SAGE Publications.
- Stat Counter, (2019). Mobile Operating System Market Share Australia Feb 2018 – Feb 2019. Retrieved from <http://gs.statcounter.com/os-market-share/mobile/australia>
- Deloitte, "Mobile Consumer Survey 2018".
- InMoment, 2018. 'What Brands Should Know About Creating Memorable Experiences'. CX Trends Report
- Business of App. (2018). APP Download and Usage Statistics. Retrieved from <http://www.businessofapps.com/data/app-statistics/>
- Enisa. (2017). Privacy and data protection in mobile applications. A study on the app development ecosystem and the technical implementation of GDPR.
- The Conversation. (2017). 7 in 10 smartphone apps share your data with third-party services. Retrieved from <https://theconversation.com/7-in-10-smartphone-apps-share-your-data-with-third-party-services-72404>
- The Verge. (2018). Apple is reportedly removing apps that share your location data with third parties. Retrieved from <https://www.theverge.com/2018/5/9/17334602/apple-targeting-apps-location-data-sharing-third-parties>
- ABC. (2019). Data sharing by popular health apps found to be 'routine', prompting calls for more transparency. Retrieved from <https://www.abc.net.au/news/science/2019-03-21/health-apps-sharing-data-common-practice-study-finds/10923484>
- eMarketer. (2018). Most Apps Get Deleted Within a Week of Last Use. Retrieved from <https://www.emarketer.com/content/most-apps-get-deleted-within-a-week>

Contacts

David Batch

National Privacy and
Data Protection Lead,
Risk Advisory
Sydney
+61 401 113 033
dbatch@deloitte.com.au

Tommy Viljoen

National Lead Partner
Cyber Strategy and Governance,
Risk Advisory
Sydney
+61 414 793 296
tfviljoen@deloitte.com.au

Daniella Kafouris

Partner, Risk Advisory
Melbourne
+61 3 9671 7658
dakafouris@deloitte.com.au

Lani Refiti

Partner, Risk Advisory
Brisbane
+61 412 306 477
lrefiti@deloitte.com.au



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

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

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

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

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte Network.

© 2019 Deloitte Touche Tohmatsu