Is an ethical approach to customer data privacy your trust differentiator?

How brands need to adapt to changing times for consumer data

The better the question.
The better the answer.
The better the world works.

EY
Building a better working world

Authored by:

Adam Fraser
Director, Business Consulting, EY

The data privacy issue straddles the enterprise … and marketers need to be part of the conversation

Handle with care

The right to use assets, especially tangible ones, is rarely an issue of debate. It tends to be a question of fact.

Yet in relation to digital consumer data post-internet, we seem to have lived through a period of ambiguity with many brands in a mindset of 'asking for forgiveness not permission'. As rapid internet growth over the past 2 decades created a new form of Wild West, and the globe slowly adjusted to new rules of engagement in a digital landscape, access to, and use of, consumer data became collateral damage in that adjustment process.

In terms of commercial use of personal data, consumer and societal attitudes have unquestioningly shifted in recent years … and brands now need to adjust to a new normal. The practices of the past are no longer acceptable.

With the aggregated value of personal data becomingly increasingly obvious over time, the data privacy genie is now out of the bottle. After a number of public scandals, brands are on notice that personal data must be handled with respect and care.
The regulators are coming, and consumers are fighting back.

Need to know

Breaching a consumer's trust is quite simply bad for business. Breach of trust damages brand equity, sales and loyalty. A business which misuses customer data will be fundamentally seen as untrustworthy and unethical. It's not where you want to be in 2020.

On the flipside, transparent and ethical data handling can build trust and brand.

If consumers want personalised customer experience and customer service, they need to provide data. To do this they need to trust the brand. In today's world, they increasingly do not. Ethical and transparent management significantly improves the likelihood that consumers feel comfortable enough to provide this data.

Data sharing, consents and preference management have become a customer experience (CX) issue as well as a regulatory one. The recent ACCC reports indicate privacy legislation will be changing in Australia, but irrespective of the detail within the legislation, this topic matters and needs attention.

Data Privacy is becoming a competitive differentiator. As an increasingly important consumer issue, marketers need to be part of this conversation, alongside their legal, risk and compliance colleagues.

Global regulators catching up

Global privacy legislation is now playing catch up to cater for the realities of a post-internet world, most notably with the launch of General Data Protection Regulation (GDPR) in Europe in May 2018 and the California Consumer Privacy Act (CCPA) in the USA taking effect from January 1, 2020. Significant legislative change is afoot across the globe.

Personal data rights are becoming entrenched where they should have always belonged – with each individual consumer. **Brands need to adjust to a world where they are data custodians using private consumer data on explicitly agreed terms.**

“

I was in a forum recently when someone talked about the person being the data owner and they were referring to someone in their team being the data owner and I said ‘no, please remember the data’s owner is the individual themselves’. They give permission to a company for a period of time to use that data, to serve up either personalised content or better offers or some other things.

We haven’t yet got to that phase, but I think through a combination of culture and regulation and technology, we’re going to get there pretty fast. Data privacy is a product and there is profit and value to be created out of data privacy ...

Clive Dickens
Optus on the EY Podcast
“Let’s Talk Marketing”

Who manages personal data in an enterprise?

This is the challenge for a typical brand – often it can be "everyone, but no one".

The issue of data governance can often straddle a number of siloed departments including inter-alia:

- IT
- Risk
- Compliance
- Legal
- Privacy
- Marketing
- Customer Service
- Data
- Insights

Accordingly, typically different departments will own part of the process, but no-one holistically manages an issue which needs to be managed horizontally across an enterprise, not vertically within a single siloed department.

Data governance and culture are critical issues in the effective and ethical management of customer data; core systems and processes need to underpin the approach, but an ethical, customer -centric culture is also required to ensure staff all buy-in to the approach and, in the event of ambiguity, take the ethical, customer focused approach to do the right thing.

> "Consumers are not adequately informed about how their data is collected and used and have little control over the huge range of data collected

Extract ACCC Digital Platforms Review

What's the story in Australia?

Australian businesses are regulated by the following pieces of legislation in the area of privacy:

- Privacy Act (1988) which includes the 13 Australian Privacy Principles
- Spam Act (2003)
- Notifiable Data Breaches Scheme (2017)
- Consumer Data Right (CDR) enacted via the Treasury Laws Amendment (Consumer Data Right) Bill 2019

The core legislation (the Privacy Act) was written in 1988 – pre internet.

In 2019 the Australian Competition & Consumer Commission (ACCC) focused on the issue of data privacy in two separate reports:

- Digital Platforms Review (June 2019)
- Customer Loyalty Schemes Review (December 2019)

In both cases the ACCC identified some serious concerns on how consumer data is being handled and used, with recommendations to address these in new privacy legislation.

It is important to note that the recommendation about broader reform of the Australian privacy regime in the later report was wholly consistent with the ACCC's recommendation in its earlier report. This is clearly a matter of focus and importance to the ACCC, and it is reasonable to expect a change in Australian privacy legislation in the near future.

> "The ACCC is of the view that the findings from this review of loyalty schemes reinforces the ACCC's findings from its Digital Platforms Inquiry, and further supports our recommendations for economy-wide changes in relation to privacy law.
>
> **Extract ACCC Loyalty Schemes Review**

How should brands react? The carrot and the stick...

A foundation of any brand is trust. A brand is a promise to deliver on an expectation. This promise relates to both the product/service experience as well as broader ethical considerations such as management of personal data.

Mis-handling consumer data – whether that be sharing it with third parties without consent or putting it to use for purposes which a consumer did not agree – can damage trust and therefore also negatively impact the strength of the brand.

In a digital era, many aspects of customer service and customer experience require personal data to drive a personalised experience. A consumer will have to trust a brand to provide that data. A transparent value exchange will be required to encourage that data provision – if I provide you with "x" my enhanced experience and utility will be "y".

Lack of trust (and lack of a transparent, defined value exchange) will equate to lack of data, which in turn can inhibit the customer experience. Conversely, transparency will drive greater data collection, enhanced trust and also avoid any nasty consumer surprises and "the creepy stalker factor" arising from unexpected brand engagement or personalised ads.

The days of collecting data for no explicit purpose (or consumers being willing to share that data for no explicit pay back) are coming to an end. And rightly so.

As indicated in the ACCC reports, behaviour to date by many brands has been sub-optimal; distrust seems to be the starting point for consumers. In this low performance playing field, ethical and transparent management of consumer data can become a competitive differentiator.

Accordingly, providing a consumer with very clear parameters around:

- why data is being collected
- how it is going to be used (to their benefit) in a very granular way
- ways by which a consumer can manage their data and preferences in real time

is a means to drive brand and CX, as well as meeting global regulatory best practice and expected potential Australian regulatory stipulations.

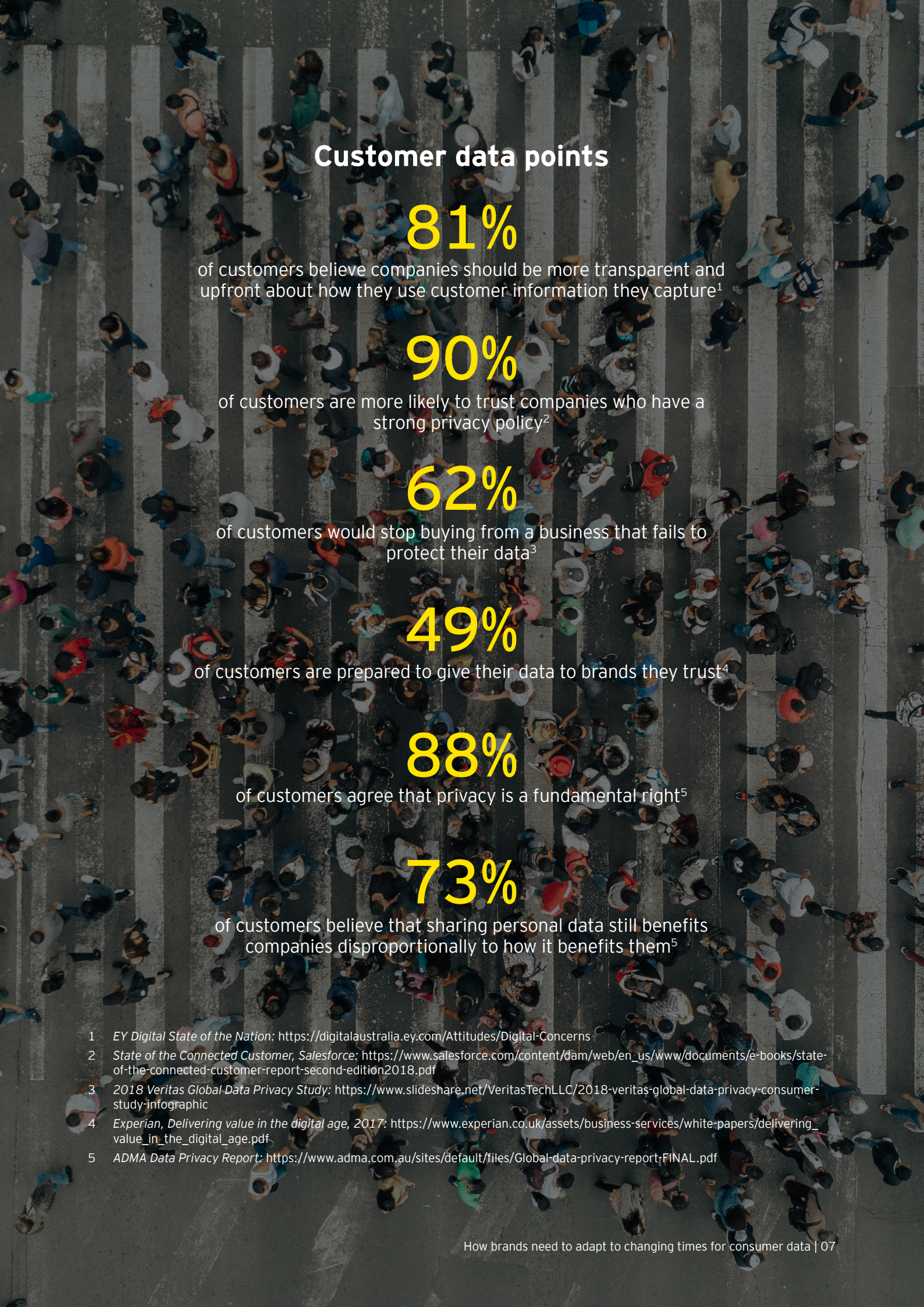
Why should marketers care?

Marketing (should) own the customer, working collaboratively across the enterprise to optimise the CX. Marketing need to drive this conversation. From plain English legal documentation (Terms and conditions, Privacy policy, Cookie policy, Notifications), transparency around data capture and use, granularity of consent frameworks, and the UX of how data is captured, marketing need to be involved. End to end. Getting this right can enhance the brand.

This issue cannot sensibly be handed purely to the risk and legal teams. This risks ignoring the Customer.

> "Symptomatic of poor data behaviour, consumers feel they need to manage their preferences

Senior marketer in a large healthcare organisation



Customer data points

81%

of customers believe companies should be more transparent and upfront about how they use customer information they capture[1]

90%

of customers are more likely to trust companies who have a strong privacy policy[2]

62%

of customers would stop buying from a business that fails to protect their data[3]

49%

of customers are prepared to give their data to brands they trust[4]

88%

of customers agree that privacy is a fundamental right[5]

73%

of customers believe that sharing personal data still benefits companies disproportionally to how it benefits them[5]

1 *EY Digital State of the Nation:* https://digitalaustralia.ey.com/Attitudes/Digital-Concerns

2 *State of the Connected Customer, Salesforce:* https://www.salesforce.com/content/dam/web/en_us/www/documents/e-books/state-of-the-connected-customer-report-second-edition2018.pdf

3 *2018 Veritas Global Data Privacy Study:* https://www.slideshare.net/VeritasTechLLC/2018-veritas-global-data-privacy-consumer-study-infographic

4 *Experian, Delivering value in the digital age, 2017:* https://www.experian.co.uk/assets/business-services/white-papers/delivering_value_in_the_digital_age.pdf

5 *ADMA Data Privacy Report:* https://www.adma.com.au/sites/default/files/Global-data-privacy-report-FINAL.pdf

Tech is putting the consumer in control

Optimising performance in this area involves managing both the downside aspect (potential regulatory breaches, fines, negative PR, brand damage as well as outside risks such as cyber-security, hacking and theft) and the upside aspect (optimising CX and building trust via ethical and transparent management of consumer data).

This necessitate a major shift in thinking.

CRM Systems and 'One view of the customer' programs were predicated on brands' ownership of the data. It belonged to the enterprise.

Technology offerings in the form of Customer Data Platforms/Clouds are based on the premise that the right to use or access private customer data is managed by the consumer, with the brand as custodian of the data for specific, mutually agreed purposes.

Best practice has the consumer being able to access:

- The data a brand possesses about them
- The uses to which that data is being put
- Granularity of their consents and preferences across multiple "use cases" for the data.

at any time, and to be able to amend their preferences at all times.

This is true customer centricity. This requires a shift in thinking, culture and core business processes. Not easy … but worthwhile. If the customer is king, and you truly are customer-centric, it's time to follow through and act this way in such an important area.

Control around access to personal private data should belong to the customer and it's a valuable asset … it's time to start acting this way.

Listening to the market

In finalising our perspective on this topic, we held a number of conversations with senior marketers in the industry, across a range of sectors.

The conversations were valuable insights into the market's response to the ACCC report and their attitudes to this topic more broadly.

The key thematics of this market input were:

- This is indeed an important topic with attention at the senior exec and board level
- This topic is increasingly important to consumers and is a huge gap in frontline marketing capability
- Any sort of data breach/error involving customer data soaks up an enormous amount of internal time and expense to fix
- Tech architecture and governance is important as consumer data can often sit across many areas of the business
- This issue is important for brand and CX – it's not just a regulatory issue.

One banking CMO we spoke to asked: If data isn't kept safe, can customers remain confident their money won't also be at risk?

> Our mission centres on being a trusted brand; approach to data privacy is critical to this hence gets board level attention and focus

Senior exec, TMT business

What's next?

You need senior management and board buy in as to the importance of this nuanced issue, in order to drive the holistic change needed to execute on global best practice. This will need a whole of enterprise response. Upside and downside considerations need to be managed.

- **Where are you now?**
  - What is the lay of the land in your business?
  - Who manages customer data and where does it sit?
  - How is customer data currently being used?
  - Is customer data being shared with third parties?
  - Do you have auditable, explicit consumer consents in all areas?
  - Do you have a customer data charter and social contract with your customers?
  - Do you allow customers to manage their own preferences and data?
- **Where do you want to get to?**
  - Map out best practice as applied to your brand
  - Hand the keys to the data to the customer – think customer preference centre
  - Think of data sharing, consent and preference frameworks as CX facilitators
  - Define the data you truly need and the value exchange with the consumer
  - Operationalise the enterprise wide changes needed
- **How will you get there?**
  - Clear ownership of topic and role definitions across the enterprise
  - Change management program with clear governance and ownership
  - Tech system implementation/optimisation
  - Business process re-engineering
  - Legal documentation consistent with charter and strategy
  - Focus on the customer and customer experience every step of the way

This topic can be a double-edged sword. The path to brand strength, enhanced trust and customer loyalty ... or a PR nightmare waiting to happen, with costly legal and operational consequences.

Intentional, proactive strategic planning in an area that previously may have been relegated to the passive and unimportant, is key. Driving the changes needed to execute personalised consumer communications based on explicit, granular preferences is complex to execute from both a technology and a business process perspective. True customer centricity does not come easy.

How can EY help?

EY can provide multi-faceted, holistic advice in the area of data privacy.

EY has multiple spheres of experience relevant to this topic including:

- Legal
- Risk
- Cyber-security
- Customer and Strategy
- Data and Analytics
- Technology
- Market research
- Project Management
- Change Management

APPENDIX: KEY INFORMATION

Personal data: GDPR, Europe

Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Key Issues: GDPR

- Harmonise data privacy laws across Europe
- Greater protection and rights for individuals
- Companies need to document lawful basis for collecting data
- Right for individuals to access and correct data held by a business about them
- Right to be forgotten
- Consent needs to be explicit
- Data breaches need to be reported within 72 hours
- Penalties of up to €20 million or 4% revenue, whichever is greater

ACCC Recommendations: Digital Platform Review

- Strengthening protections in the Privacy Act
  - Update definition of "personal info"
  - Strengthen notification requirements
  - Strengthen consent requirements and pro-consumer defaults
  - Enable erasure of personal information
  - Introduce direct rights of action for individuals
  - Higher penalties for breach of the Privacy Act
- Broader reform of the Australian privacy law framework
  - Higher standard of protections
  - Inferred information
  - De-identified information
  - Overseas data flows
  - Third party certification
- The introduction of a privacy code of practice specifically for digital platforms
- The introduction of a statutory tort for serious invasions of privacy
- Revisit the applicability of the CDR to digital platforms in the future.

Personal Information: Privacy Act, Australia

Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

Key Issues: CCPA

- Designed to protect the data privacy rights of citizens living in California
- Forces companies to provide more information to consumers about what's being done with their data
- Gives consumer more control over the sharing of their data
- A right to know (or "transparency") about how the data is being used, a right to access, and a right to opt-out of having their data sold to third parties.

ACCC Recommendations: Loyalty Schemes Review

- End the practice of automatically linking members' payment cards to their loyalty scheme profile
- Improve the data practices of loyalty schemes via:
  - Reviewing clickwrap agreements for unfair contract terms
  - Improving the clarity, accessibility, navigability and readability of privacy policies
  - Minimising information overload for consumers
  - Outlining clearly with which entities consumer data is being shared and for what purposes
  - Drawing to consumers' attention how their data is being handled
  - Disclosing to consumers the sources of third party advertising, consumer data used to inform that advertising, and the channels through which they may receive targeted advertising
  - Providing consumers with more meaningful controls over the collection, use and disclosure of their data

Contacts

Adam Fraser
Director | Advisory
Ernst & Young Australia
adam.fraser@au.ey.com

Charlie Offer
Partner | Risk | Advisory
Ernst & Young Australia
charlie.offer@au.ey.com

Frith Tweedie
Director | Digital Law
Ernst & Young New Zealand
frith.tweedie@nz.ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation is available via ey.com/privacy. For more information about our organization, please visit ey.com.

APAC No. AUNZ00001233
ED none.
PH1014579

ey.com/au