



Consumer data and the digital economy — summary report

Emerging issues in data collection, use and sharing

Phuong Nguyen & Lauren Solomon



Big Data and consumers

Significant benefit and innovation can flow from open data. To deliver sustainable growth of new technologies and industries, it's crucial that we put consumers in the driver's seat.

Australians are spending more of their lives online. 87% were active internet users in 2017¹, more than 17 million use social networking sites², and 84% of Australians are now buying products online³.

Big Data is big business. In 2018 alone, revenue from the Big Data software market was estimated at \$42 billion⁴.

The introduction of the General Data Protection Regulation now provides EU consumers with new protections including greater transparency and control of data being collected about them by companies.

In Australia, consultation is currently underway to establish a Consumer Data Right, an optional right for consumers to gain access to portability of their data. While a step in the right direction, it currently falls short of economy-wide protections for Australian consumers whose data is being collected, shared and used on a daily basis.

Ensuring that we strike the right balance is crucial. For consumers to benefit, policy settings need to drive innovation, enhance competition, protect human rights and the right to privacy and, ultimately, enable genuine consumer choice.

Big Data, big growth

We are generating more data than ever before. A recent report from Forbes highlights the massive global growth of Big Data through everyday activities⁵.

- Over the last two years alone 90% of the world's data was generated
- More than half of all web searches are now conducted from a mobile phone
- Google now processes more than 40,000 searches every second
- Facebook had more than 2.2 billion active users as at Q1, 2018
- We send 16 million text messages every minute

1. Statista. (2018a). Active internet users as percentage of the total population in Australia from 2015 to 2017. Statista. Available at <https://www.statista.com/statistics/680142/australia-internet-penetration/>. (Accessed on 24 January 2018)

2. Statista. (2018b). Number of social network users in Australia from 2015 to 2022 (in millions). Statista. Available at <https://www.statista.com/statistics/247946/number-of-social-network-users-in-australia/>. (Accessed on 24 January 2018)

3. Office of the Australian Information Commissioner (OAIC). (2017a). Australian Community Attitudes to Privacy Survey 2017. Office of the Australian Information Commissioner, Sydney, Australia. Retrieved from <https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017>.

4. Columbus, L. (2018). 10 Charts that will change your perspective of Big Data's Growth. Forbes. Available at "<https://www.forbes.com/sites/louiscolombus/2018/05/23/10-charts-that-will-change-your-perspective-of-big-datas-growth/>"<https://www.forbes.com/sites/louiscolombus/2018/05/23/10-charts-that-will-change-your-perspective-of-big-datas-growth/#41666c329268>. (Accessed 30 May 2018).

5. Forbes (2018). How much data do we create every day? The mind-blowing stats everyone should read. Available at: <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#4669ba6f60ba>. (Accessed on 9 July 2018).

Opportunities and risks

Opportunities

Improving health and wellbeing

Big Data enables artificial imaging for skin cancer, artificial intelligence to assist the hearing impaired, smart-glasses for the visually impaired, and real time feedback from sensorised prosthetics to improve experience.

Fraud detection

More granular analysis of accounts enables quicker identification of fraudulent activity, which reached \$540 million* AUD for cheques and cards in 2016⁶.

Improving efficiency and processes

Big Data enables more effective investment in urban planning, public transport and healthcare services, as well as real time monitoring of energy and water usage.

Access to more suitable products

Greater access to and portability of consumer data can enable more accurate recommendations and tailoring of products to suit needs.

More relevant advertising

Consumers can receive more relevant information about the products and services that better match their needs.

Competition enabler

Opening up consumer data to be accessed and ported can act as a competition enabler, reducing the amount of data that is held with only one supplier or entity.

Risks

Loss of privacy

Significant amounts of data are now being collected about consumers' movements, connections, preferences, and behaviours. There are often extremely limited options available to consumers who would like to choose to limit the collection and transfer of their data.

Consumer profiling and scoring

Increasing evidence of profiles and scores being developed of consumers, based on everything from browsing history, likes on social media, shopping behaviour, to the purchase of information from data brokers. Currently, there is little to no transparency for consumers.

Increasing scope for price discrimination

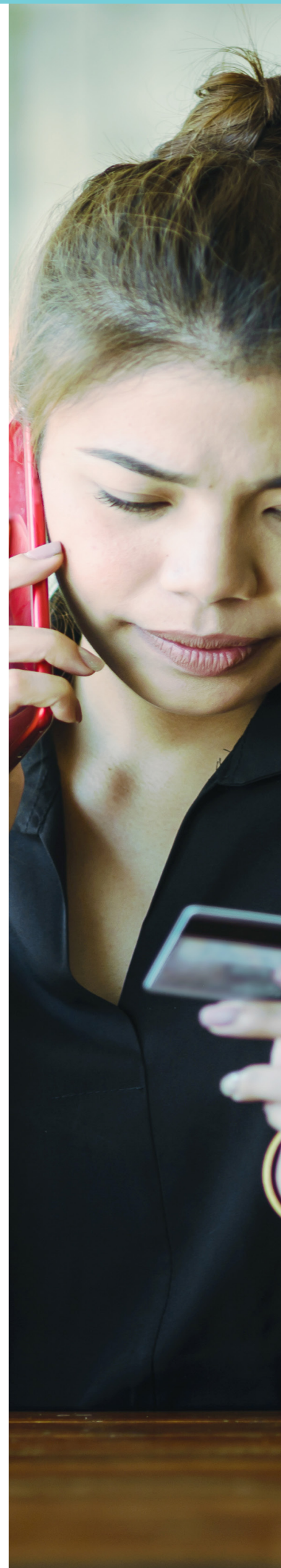
More granular data on consumers is being used to develop profiles and, in turn, to offer different prices for the same product to different consumers. This increases the potential for a shift from *third degree* to *first degree* price discrimination.

Exclusion from products & services

Several cases have been uncovered internationally of consumers being excluded from certain products and services, based on their 'profile'. This is of significant concern for essential services.

Algorithms perpetuating bias and discrimination

Algorithms powering profiles and scores can be built on data that is either: error-filled; wilfully provided incorrectly; and/or biased. Without greater transparency, algorithmic profiling practices run the risk of embedding discrimination and exclusion.



6. Australian Payments Network. (2017). Australian Payments Fraud 2017. Jan-Dec 2016 Data. Australian Payments Network. Retrieved from https://www.auspaynet.com.au/sites/default/files/2018-01/australian_payments_fraud_details_and_data_2017.pdf.

*Statistics updated from previous version of CPRC report (updated 17th July 2018)

Australian attitudes, knowledge and preferences

CPRC engaged Roy Morgan Research to conduct a nationally representative survey of 1004 Australians throughout March to April 2018, along with two focus groups. These findings demonstrate the gap between community expectations and current practice in the Australian digital economy.

Australians value their privacy

Australians were largely uncomfortable with companies sharing their data with third parties for purposes other than delivering the service.

Consumers were most uncomfortable sharing information about others (such as phone contacts and messages) or information about their personal devices (phone numbers and unique IDs). See Figure 1.

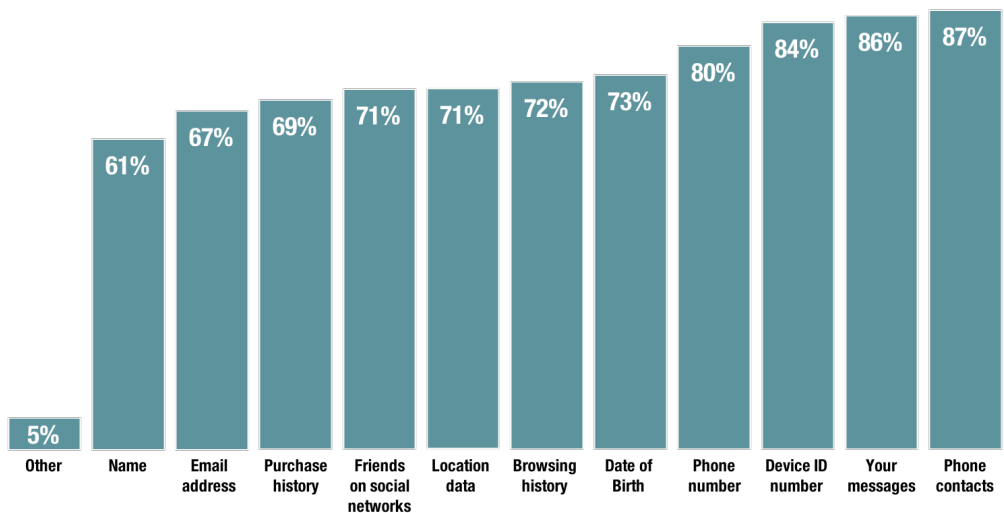


Figure 1. What data/information would you be uncomfortable with companies sharing with third parties for purposes other than delivering the product or service? (Select all that apply)

Privacy policies are not providing consumers with adequate control

Of the 67% of Australians surveyed who reported reading a Privacy Policy or Terms and Conditions for one or more services/products they signed up to in the past 12 months, two-thirds indicated that they still signed up for one or more products even though they did not feel comfortable. See Figure 2.

The most common reason (73%) for accepting privacy policies with which consumers were not comfortable was that it was the only way to access the product or service.

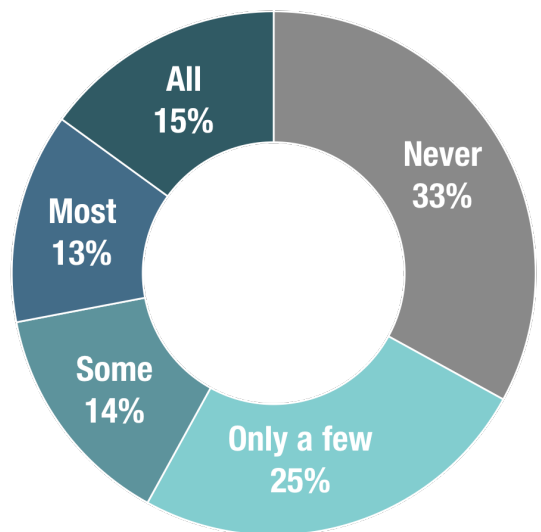


Figure 2. In the past 12 months, how often did you 'accept' a company's Privacy Policy or Terms and Conditions to use a product or service, even though you did not feel comfortable with the policies?

Australian consumers expect their data to be used fairly by companies

The Australian expectation of the 'fair go' was certainly found to apply to data practices. Consumers surveyed found it unacceptable for companies to: charge different consumers different prices based on their profile (88%); collect data about them without their knowledge to assess eligibility or exclude from a loan or insurance (87%); or use payment behaviour data to exclude from certain essential products and services (82%). See Figure 3.

Consumers clearly want to be provided with greater transparency and control over data collection sharing and use practices.

Of those surveyed:

- › 95% wanted companies to give them options to opt out of certain types of information collected about them, how it can be used and/or what can be shared with others.
- › 91% agreed that companies should only collect the information currently needed to provide the service.
- › 92% wanted companies to be open about how they use data to assess eligibility.

Charge different prices for the same product in the same hour, based on past purchasing, online browsing history, or payment behaviour?

11%

77%

Collect data about you without your knowledge to assess eligibility or exclude from a loan or insurance?

11%

76%

Collect data about payment behaviour to assess eligibility or exclude from essential products & services (e.g. electricity, gas, telecommunications)?

14%

68%

■ Somewhat unacceptable ■ Very unacceptable

Figure 3. How acceptable or unacceptable do you find it for companies to use your data to...?

Consumers want better protections

There is a clear expectation from Australian consumers that policymakers should act to protect their privacy; deliver greater optionality when it comes to what data is collected, shared and used; and ensure that consumers are not unfairly excluded as a result of their data or profile. See Figure 4.

It should be my data, I should have rights to it.

Focus group participant

The Government should ensure companies give consumers options to opt out of what data they provide, how it can be used, and if it can be shared with others

73%

The Government should develop protections to ensure consumers are not unfairly excluded from essential products or services based on their data and/or profile

67%

Figure 4. What role do you think government has in regulating how companies use your data? (Select all that apply).



Policy implications

In a period of rapid technological transformation, ensuring the surrounding policy and regulatory environment is agile is essential. Environment scanning for emerging technologies, applications and issues are key, along with added protections to ensure innovation is sustainable and in line with consumer and community expectations.



Building consumer trust and confidence to participate in the digital economy

Policy and regulatory settings must ensure that consumers can build trust through their participation in the digital economy. This will be central to the sustainable development of innovative technologies that are dependent on data collection.

The United Kingdom's Competition & Market Authority provides useful guidance for businesses and government on the elements of consumer data use practices that support well-functioning markets; which includes⁷:

- › Consumers know when and how their data is being collected and used; and have some control over whether and how they participate.
- › Businesses are using the data to compete on issues that matter to the consumer.
- › The use of consumer data benefits both consumers and businesses.
- › Rights to privacy is protected through the regulation of data collection and use.
- › There are effective ways to fairly manage non-compliance with regulation.



Consumers need to be provided with genuine choice & control over collection, sharing & use

Reforms to ensure that consumers are put in the driver's seat when it comes to their own data are critical. Protections and regulations that are reliant on a consent model must ensure consumers genuinely comprehend and have choice over the type of data being collected, who it is being shared with and for what purpose.

Comprehension testing and behavioural research should inform consent requirements.

Essential elements of any consent regime must ensure that the consent provided is⁸:

- › Expressed – the controller must be able to demonstrate that consent was given.
- › Specific to purpose (unbundled with other matters).
- › Easy to understand (written in clear and plain language).
- › Easily accessible
- › Able to be withdrawn (as easily as it is to give consent).
- › Freely given (not conditional if the data is not necessary for the provision of the service).



Ensuring consumers' right to privacy is adequately protected

Experts caution against a wholly self-management approach to privacy⁹.

A balanced approach includes: having a definition for valid consent; developing practical mechanisms for people to manage their privacy for all entities, rather than micro-managing each; adjustment of time and focus of privacy law to provide guidance on types of uses at the time they are proposed; and the law to develop a code of basic privacy norms⁹.

Privacy by Design principles can be also applied by businesses and regulators to protect consumer privacy during the design phase, and throughout the lifecycle of any product^{10, 11}.

7. Competition & Markets Authority (CMA). (2015). The commercial use of consumer data: Report on the CMA's call for information. Competition & Markets Authority, London, United Kingdom. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf

8. Intersoft consulting. (n.d.b). Art. 7 Conditions for Consent. Intersoft consulting. Available at <https://gdpr-info.eu/art-7-gdpr/> (Accessed 17 April 2018).

9. Solove, DJ. Introduction: Privacy self-management and the consent dilemma. Harvard Law Review. 2013, 126 (7): 1880-1903



4 Greater transparency of, and access to data and profiles

Enabling greater transparency and access to the scores and profiles that are being built of consumers can help to avoid incorrect, biased and potentially discriminatory practices. Without transparency for consumers as to what data may have been used as an input to a company making a decision, they are unable to either challenge the outcome nor change their behaviour in the future to achieve a different outcome.

To ensure algorithms and scores are not discriminatory, regulators can increase monitoring, auditing and assessment powers. Examples of algorithmic auditing and assessment services emerging internationally include bias check services established by the Algorithmic Justice League and ORCAA established by mathematician Cathy O'Neil for companies to test the fairness of the algorithms they are using^{12, 13}.



5 Strengthening regulatory monitoring and intervention powers

The evolution of technology and machine-learning practices require a significant shift in capability, skills and monitoring powers within regulators.

It is critical that regulators are adequately resourced and skilled to keep pace with new technologies and practices. They also need to be armed with sufficient discovery powers to identify potentially discriminatory or predatory lending behaviours, based on profiling practices, and to audit or assess algorithms. This will require investment in new skills, systems and people to keep pace with a fast-moving commercial environment.

Ensuring the academic and community sector are also sufficiently resourced to engage in policy and regulatory development processes will be key during this economy-wide shift in the operation of our markets.



10. Information and Privacy Commissioner of Ontario (IPC). (2013). Privacy by design. Information and Privacy Commissioner of Ontario. Available at <https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf>. (Accessed 8 May 2018)
11. Information Commissioner's Office (ICO). (2018). Data Protection by design and by default. Information Commissioner's Office Available at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/>. (Accessed 6 July 2018)
12. Algorithmic Justice League. (2017). Algorithmic Justice League. Available at <https://www.ajlunited.org/>. (Accessed 30 May 2018)
13. ORCCA. (n.d.). O'Neil Risk Consulting & Algorithmic Auditing. ORCAA. Available at <http://www.oneilrisk.com/>. (Accessed 30 May 2018)



Level 14, 10-16
Queens Street

Melbourne
Victoria 3000

T 03 9639 7600
F 03 9639 8966

cprc.org.au
ACN 100 188 752



**Consumer
Policy Research
Centre**