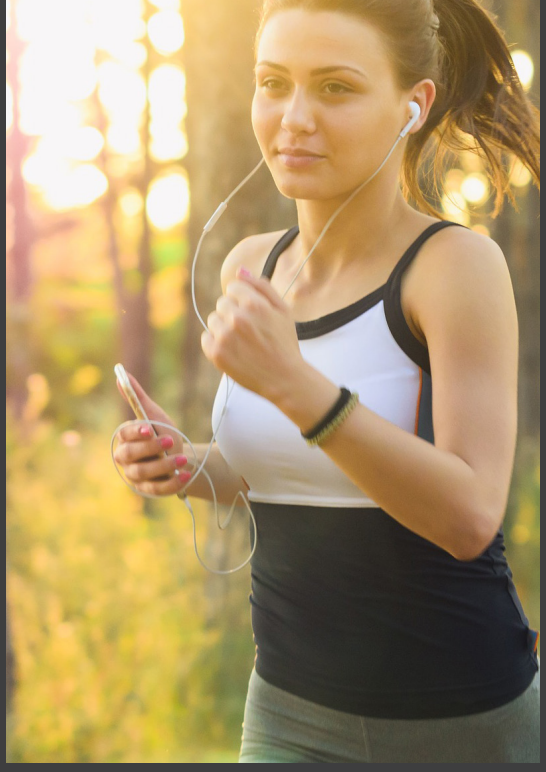
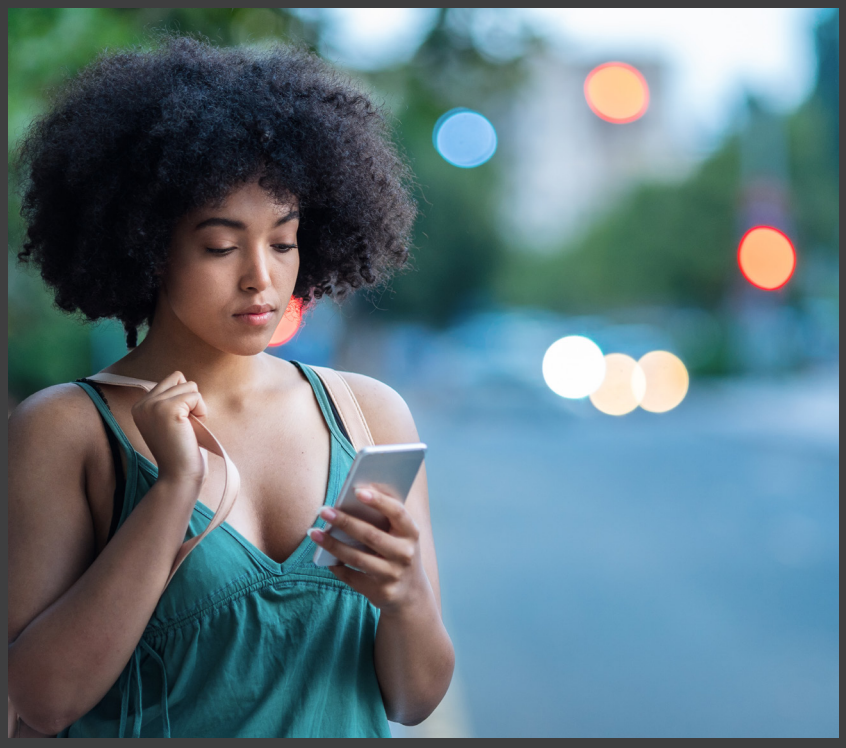




Consumer Policy Research Centre

A Day in the Life of Data

Removing the opacity surrounding the data collection, sharing and use environment in Australia

Brigid Richmond

ABOUT CONSUMER POLICY RESEARCH CENTRE (CPRC)
CPRC is an independent, non-profit, consumer think-tank established with seed funding by the Victorian Government in 2016. CPRC undertakes consumer research independently and in partnership with others to inform evidence-based policy and business practice change. We work closely with policy makers, regulators, academia, industry and the community sector to develop, translate and promote evidence-based research to inform practice and policy change. To find out more visit www.cprc.org.au.

Acknowledgements

CPRC has engaged data trust, data ethics and data privacy firm Greater Than X to deliver some sections of this report, which have been attributed accordingly. CPRC engages external organisations on projects where:

- The organisation meets CPRC Funding and Partnerships Policy requirements.
- We share the same research goals for the project.
- The necessary skills, knowledge and expertise to complete the project requires collaboration.

CPRC supports effective competition in services to improve outcomes for consumers. In no way does this engagement imply endorsement, support, or advocacy for Greater Than X services and activities beyond the information provided in this report. We are very grateful for the contributions made by the Greater Than X team Nathan Kinch, Mathew Mytka and Nadia Lee, and the cross-sectoral knowledge shared in delivering this project.

Key findings 3

Introduction 4

The data collection landscape 6

Your life in data 13

Privacy policies 25

Harms 34

Policy responses 41

Better business practices 49

Conclusion 53

References 55

Appendices 59

Key findings

1 **Data tracking is increasingly inescapable.** Trackers are common offline and online. Even non-users of major services such as Google and Facebook have been found to be tracked by those companies.

2 **The data collection landscape is largely opaque**. Consumers don't understand what they are handing over or the value of that data. Policy makers will find it difficult to design effective remedies unless the supply chain governing data collection, sharing and use is more transparent.

3 **Consumers feel overwhelmed** by privacy policies and have limited understanding or control over their personal data.

4 **Targeted advertising is not the major harm.** The more significant harms – and the harms that policy makers and regulators should be discussing – are the growing risks of consumer manipulation, discrimination and exclusion based on automated decision-making using online and offline profile data.

5 **Transparency and accountability are key.** Key issues for policy makers include: requiring transparency, enabling consumer comprehension and control, implementing accountability measures (for data collection and for automated decision-making), establishing minimum protection standards and preventing exploitation.

Introduction

The promise of data

Digital disruption is occurring at a rapid pace, creating significant change before regulators, governments, or consumers have had a chance to grapple with the consequences. This has predominately been a technology-led and industry-led environment, with firms often the ones determining the new "norms" while policy makers play catch up. The promises of the Fourth Industrial Revolution, built on the presumption of access to large scale data, contain massive benefits for Australians as well as risks.

Ideally, an innovative Australia embracing technological developments would create value that has broad social and economic benefits. One example is the possible use of insights from bank transactions to identify and assist victims of economic abuse.[1] The challenge is to ensure potential benefits are realised, and the risks – such as exacerbated social inequality and exclusion – are avoided.

This won't be possible without consumers trusting data collection, sharing and use practices. Opaque business practices and undisclosed data sharing arrangements do not encourage trust. Transparency and implementing minimum protection standards will be two key levers for building that trust, by supporting informed consent and enabling consumers to identify the benefits for themselves and for Australia.

Recognising these challenges, regulators and policy makers internationally have turned their attention to reforming policy frameworks and encouraging ethical innovation, including the acceptable uses of consumer data. It is now time for Australia to join the discussion. This report is intended to shine a light on current data collection, sharing and use practices underway in our daily lives as Australian consumers, explore potential harms, and the actions that policy makers and businesses can take to better empower consumers.

The data collection landscape

Consumers today are tracked online and offline by a range of technologies and organisations that share that information with each other and data brokers to create online customer profiles. Online business models are increasingly oriented towards data collection, with an estimated 91% of the top one million websites tracking their visitors.[2] Zuboff terms this environment "surveillance capitalism", where human experience is the "free raw material for hidden commercial practices of extraction, prediction and sales".[3] The profiles created can be used to predict and influence consumer behaviour as well as support automated decision-making with humans, according to the historian Yuval Noah Harari, "…becoming tiny chips inside a giant data processing system that nobody really understands".[4]

1. Batagol, B and Neave, M (1 February 2019) "Banks are Enabling Economic Abuse. Here's How They Could Be Stopping It" The Conversation (https://theconversation.com/banks-are-enabling-economic-abuse-heres-how-they-could-be-stopping-it-110439)
2. Libert, T Cylab Security and Privacy Institute, Carnegie Mellon University, quoted in Marechal, N. (17 November 2018) "Targeted Advertising is Ruining the Internet and Breaking the World" Motherboard (https://motherboard.vice.com/en_us/article/xwjden/targeted-advertising-is-ruining-the-internet-and-breaking-the-world)
3. Zuboff S. (2019) The Age of Surveillance Capitalism, New York: Hatchette Book Group, quoted in Ross, A. "How Big Tech Built the Iron Cage," New Yorker, (https://www.newyorker.com/culture/cultural-comment/building-the-digital-iron-cage)
4. Harari, Y.N. (2018) Twenty-one lessons for the Twenty-First Century, UK: Penguin Random House, p.56

Opaque business practices and unintelligible privacy policies mean that consumers often don't know what they are giving away to these services, their partners and affiliates, or the value of that data.

The provision of free services in return for behavioural and other data is often positioned as a fair exchange. However, research suggests that consumers do not see it that way. Consumer research conducted on behalf of the CPRC found that Australians do not fully understand the level of information being collected about them and that consumers want greater transparency and more control over how companies collect, use and share their data.[5] International research found that Americans were simply "resigned" to giving away their data in return for services. Over half of the respondents did not want to lose control of their own data but believed that it had already happened.[6]

Manwaring states that this environment means:

- A massive increase in the information collected or inferred about individual customers.
- Marketers increasingly know the combination of factors that will lead to a purchase and the customers that are most profitable.
- Customers can be targeted by marketers in a wide range of diverse situations.
- Consumers have limited understanding of what information they are sharing, the inferences made about them based on that data, or how this online profile will be used.[7]

This research report aims to remove some of the opacity surrounding the data collection, sharing and use environment in Australia.

This report

This research aims to remove some of the opacity surrounding the data collection, sharing and use environment in Australia. The report provides an overview of the data collection, sharing and use environment showing the typical flow of information from the user, the types of information collected, and inferences often made by companies based on that data. Eight privacy policies are analysed to assess readability, the data collection and sharing arrangements contained in those policies and the level of privacy controls available to consumers.

Consumer perspectives and reactions to data collection, sharing and use are also explored. Complementing CPRC's own research from 2018, this qualitative research conducted by Greater Than X demonstrates consumers feel that they lack control over their data and do not understand what data collection is occurring. On-the-street interviews conducted by the CPRC over March 2019 echo the findings of this qualitative research.

The report then examines some of the potential harms resulting from these data collection, sharing and use practices. While targeted advertising may be annoying, the real risks are discrimination, exclusion and manipulation. Policy responses, including requirements for transparency, greater consumer control, and accountability are key concerns for any government or regulator reviewing data practices and appropriate protections. Lastly, Greater Than X looks at better business practices that can be implemented to complement policy changes.

5. Nguyen P. and Solomon L. (2018) Consumer Data and the Digital Economy, Melbourne: Consumer Policy Research Centre, pp.3-4 (http://cprc.org.au/2018/07/15/report-consumer-data-digital-economy/)
6. Turow, J. Hennessy, M. and Draper, N. (2015) "The Tradeoff Fallacy: How Marketers and Misrepresenting American Consumers and Opening Them Up to Exploitation" SSRN Electronic Journal, 10.2139/ssrn.2820060
7. Manwaring, K. (2017) "Will emerging technologies outpace consumer protection law? The case of digital consumer manipulation" Competition & Consumer Law Journal, 26, p.13

The data collection landscape

The supply chain of the data collection landscape is opaque for a range of reasons, including the complexity of the processes involved and commercial sensitivity concerns.[8] Companies are not transparently or comprehensibly disclosing the data collection that is taking place. CPRC looked at the data collection landscape in partnership with Greater Than X.

According to the New York Times, in 2015 Apple found Uber identifying and tracking user iPhones even after the app had been deleted from the device.[9] Online platforms are also tracking individuals that are not using their services. For example, Google and Facebook track users who do not hold accounts with those services. Both platforms have reportedly purchased credit card transaction data and other offline activity information to enhance the online profiles of consumers.[10]

The data collection sector is now a behemoth that interacts in all parts of our daily lives. Online services have adopted an attention model, where free services or entertainment are provided, and the user's attention is then sold onto advertisers.[11] Collection of user data is embedded into the architecture of the web – through browsers and apps – and the business models of online services as a way to capture attention, increase engagement and ensure an ongoing flow of user data generation. Behavioural and other data collection activities are big business. For example, advertising based on the user's location is estimated to generate US$21 billion in 2019.[12]

Current data collection and sharing overview

Users are regularly tracked in their online interactions. The latest update provided in 2019 by WhoTracks.me, a website that has the largest dataset of monitoring trackers online, found that 81% of web traffic has Google trackers, and 28% has a hidden Facebook pixel.[13] Mobile apps also contain trackers. 2018 research analysing US and UK Google Play stores found that most of the 959,000 apps analysed contained third party trackers, with news apps and apps targeted at children having the highest number of trackers.[14]

8. Manwaring, K. (2017) "Will emerging technologies outpace consumer protection law? The case of digital consumer manipulation" Competition & Consumer Law Journal, 26, p.4
9. Isaac, M. (23 April 2017) "Uber's CEO Plays With Fire" The New York Times (https://www.nytimes.com/2017/04/23/technology/travis-kalanick-pushes-uber-and-himself-to-the-precipice.html)
10. Marechal, N. (17 November 2018) "Targeted Advertising is Ruining the Internet and Breaking the World" Motherboard (https://motherboard.vice.com/en_us/article/xwjden/targeted-advertising-is-ruining-the-internet-and-breaking-the-world)
11. Harari, Y.N. (2018) Twenty-one lessons for the Twenty-First Century, UK: Penguin Random House, p 77
12. Valentino-DeVries, J., Singer, N., Keller, M.H. and Krolik, A. (10 December 2018) "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," The New York Times. (https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html)
13. Cliqz, (14 May 2019) WhoTracks.me, https://whotracks.me/
14. Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T. and Shadbolt, N. (27-30 May 2018) "Third party tracking in the mobile ecosystem" WebSci '18, DOI https://doi.org/10.1145/3201064.3201089

Research presented at the Network and Distributed Systems Security (NDSS) Symposium in 2018 by a group of researchers from universities and scientific research centres found that 39% of advertising and tracking services analysed were cross-device tracking services[15], meaning that a substantial proportion of these services can identify the same users across multiple devices (iPad, computer, mobile, etc.). One example of such cross-technology tracking is phone software that enables monitoring of television watched by the same user across television and a smartphone.[16]

Research found that 39% of advertising and tracking services analysed were cross-device tracking services[15], meaning that a substantial proportion of these services can identify the same users across multiple devices.

Individuals are increasingly being tracked offline as well. Some shopping centres and bricks-and-mortar stores are installing beacons to track customer behaviour in the offline world.[17] Smart products, including fitness trackers and home assistants, are also tracking and storing customer data.[18] The LA Times reported that Google tracks the amount of purchases people made in bricks-and-mortar stores after clicking on an online ad in its Google services. Individuals signed into Googles services will have their combined ad clicks matched to collective purchases.[19]

Many firms then also share the data collected with partners through data sharing relationships, or this is exchanged, bought or sold via data brokers. Data brokers are increasingly extracting value from this "data exhaust"[20] of our everyday interactions, translating the raw information into behavioural models and products that can predict a user's behaviour, often unbeknownst to consumers themselves.

Data collected

Information collected can include:[21]

- Personal information (e.g. name, date of birth),
- Contact information (e.g. phone number, email address),
- Technical information (e.g. device ID, IP address),
- Location information,
- Online behaviour (e.g. search history, website visits),
- Visits to bricks-and-mortar stores, including frequency and length,
- Transactions,
- Conversations in the home logged by a home assistant,
- Biometric information (e.g. stress levels, sleep patterns), and
- Other potentially sensitive data (e.g. health information).

Companies use personal identifiers – such as smartphone IDs and phone numbers – to identify users and combine profiles across platforms, services, devices and situations.

15. Razaghpanah, A. Nithyanand, R. Vallina-Rodriguez, N. Sundaresan, S. Allman, M. Kreibich, C. and Gill, P. (18-21 February 2018) "Apps, Trackers, Privacy and Regulators. A Global Study of the Mobile Tracking Ecosystem," Conference paper, Proceedings of Network and Distributed Systems Security (NDSS) Symposium 2018, (http://eprints.networks.imdea.org/1744/)
16. Manwaring, K. (2017) "Will emerging technologies outpace consumer protection law? The case of digital consumer manipulation," Competition & Consumer Law Journal, 26, p.7
17. Hanley, G (15 December 2017) "If you go down to the mall today, you're watched by a thousand eyes" The Sydney Morning Herald (https://www.smh.com.au/technology/if-you-go-down-to-the-mall-today-youre-watched-by-a-thousand-eyes-20171211-h02h9q.html)
18. Zuboff, S. (2019) The Age of Surveillance Capitalism. New York: Hatchette Book Group, p.10
19. Associated Press. (23 May 2017). "Google starts tracking offline shopping – what you buy at stores in person," Los Angeles Times, (https://www.latimes.com/business/technology/la-fi-tn-google-ads-tracking-20170523-story.html)
20. Naughton, J. "'The goal is to automate us': welcome to the age of surveillance capitalism," The Guardian, (https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook)
21. Information collected from: Christl, W. (June 2017) "Corporate Surveillance in Everyday Life" Cracked Labs. pp. 11 – 24 and pp.49-50 (https://crackedlabs.org/en/corporate-surveillance); Editorial Board (2 February 2019) "How Silicon Valley Puts the 'Con' in Consent," The New York Times, (https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html); Vlahos, J. (26 March 2019) "Smart talking: are our devices threatening our privacy?" The Guardian (https://www.theguardian.com/technology/2019/mar/26/smart-talking-are-our-devices-threatening-our-privacy); and Manwaring, K. (2017) "Will emerging technologies outpace consumer protection law? The case of digital consumer manipulation," Competition & Consumer Law Journal, 26, p.6

Consumer profiles are created

Some companies gather, combine and amalgamate significant amounts of data to generate and store a full consumer profile. In other contexts, separate profiles of the user held by different data holders will be combined temporarily for a specific interaction, such as the delivery of advertising to a website. These profiles include information gathered from directly tracking consumers, such as search histories, and inferred information based on that data, such as interests, income and education level. 2014 research from University of Melbourne showed that mobile phone sensors can infer physical and psychological indicators, including mood, stress levels, relationship status, gender and age.[22]

In specific interactions, an enhanced profile can be used to:

- Determine the content, advertisements or products shown to a user,
- Choose the appropriate behavioural techniques to nudge a user, and
- Shape the treatment of a user, such as whether they are excluded from an offer or are singled out.[23]

Infographic 1 (p9) displays a standard process of data collection and amalgamation when searching, choosing and purchasing a simple gift online. This infographic uses the technical experiment conducted by Greater Than X as a use case to show how data is collected in our everyday lives, distributed to various players, and then used for a range of purposes, including inferring consumer attributes and delivering advertising.

Data brokers

There are many data brokers that act as the intermediary in the data collection, sharing and use process. These data brokers hold customer databases with a variety of information including demographic, credit and behaviour data, that can be used for targeted advertising, identifying high worth customers, and other uses. Many firms that consumers interact with on a daily basis have data sharing arrangements with these services.

Extremely little focus has been placed on the operation of data brokers to date in Australia, despite their central role in exchanging and combining personal information and data across a range of sectors. In 2014, the US Federal Trade Commission conducted a major investigation into the operation of data brokers, finding that: consumer data is collected from a range of sources often without consumers' knowledge; the data broker industry is complex with brokers sharing data with each other; offline and online consumer data is combined in order to advertise to those consumers online; billions of data elements are stored and cover almost all US consumers; and, that this market arrangement carries benefits and risks for consumers.[24]

More recently, in a 2019 Congress Committee's Subcommittee hearing on "Small Business Perspectives on a Federal Data Privacy Framework", Senator Blumenthal raised concerns about data brokers' business models built on detailed consumer profiles and advocated for banning the selling of customer information to third-party data brokers.[25] In the UK, the Competition and Markets Authority has recommended that a market study be conducted into the digital advertising market across the entire supply chain, including the use of consumers' personal data.[26]

22. Manwaring, K. (2017) "Will emerging technologies outpace consumer protection law? The case of digital consumer manipulation" Competition & Consumer Law Journal, 26, p.6
23. Christl, W. (June 2017) "Corporate Surveillance in Everyday Life" Cracked Labs, p.66 (https://crackedlabs.org/en/corporate-surveillance)
24. Federal Trade Commission (May 2014) Data Brokers A Call for Transparency and Accountability, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf
25. Cedarbaum, J G Nahra, K J and Freeman, Jr. D R (3 April 2019) "United States: Senate Subcommittee considers small business perspectives on a Federal Data Privacy Framework" Mondaq (http://www.mondaq.com/unitedstates/x/795444/Data+Protection+Privacy/Senate+Subcommittee+Considers+Small+Business+Perspectives+On+A+Federal+Data+Privacy+Framework)
26. UK Government (2019) "Unlocking Digital Competition" p.15 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf

Infographic 1: The Personal Data Ecosystem

Jane
shops for Valentine's Day

Name: Jane Smith
Age: 32
Gender: Female
Income: 85k
Marital status: Engaged

TYPE OF DATA

- Personal Data
- Identifiable Data
- Anonymised Data
- Re-Identifiable Data
- Targetable Data

Search engine / web browser	Online travel retailer	Social media platform	Online travel retailer	Online payment system	Credit card	Telco / vendor	Email provider	Online calendar	END? DATA COLLECTED
• Search history • Cookies tracking • Relationship • Location data • Behavioural data	• User "consent" • Behavioural data	• Financial status • Purchase and viewing behaviour • Location data	• Financial status • Purchase behaviour • Behavioural data	• Email • First / last name • Mobile number • Address / area	• Credit card info • User "consent" • Payment preference	• Sociability • Schedule • Location data • Relationship status	• Email • Transaction record • Payment preference	• Personal schedule • Relationship and financial status	

searching for present via search engines and travel retailers on the Internet

choosing present (travel tickets) by looking at travel retailers and social media platforms

purchasing present via an online payment system using her credit card on her smartphone

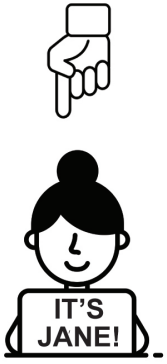
receive purchase confirmation via email and enter travel dates into online calendar

300+ PARTIES

receive data decoupled with "identifiable" information (e.g. name, email), including:

DATA BROKERS | **DATA MANAGEMENT PLATFORMS** | **DATA ANALYTICS COMPANIES** | **CREDIT REPORTING AGENCIES** | **ONLINE PLATFORMS**

who then match and aggregate the data with timestamps, IP addresses, browser fingerprints, and web visit history, which tells us that...



and the cycle continues...

Source: Greater Than X

Table 1 outlines some examples of major data brokers, their activities and partners.

Table 1: Selected Data Brokers

Data Broker	Description	Example relationships
Acxiom	Acxiom states that it tracks around 1,500 demographic, social and lifestyle data points and advertises that it has the capability to provide information and insights on over 700 million consumers around the world. Acxiom has over 400 direct customers and collects data from more than 1,000 companies through partner and reseller relationships.[27]	**Facebook:** Until March 2018, Facebook used Acxiom data to support ad targeted advertising options within Facebook.[28] Facebook shut these types of partnerships down after the Cambridge Analytica scandal. In 2017, Acxiom had partnerships with over 100 online publishers and digital marketing platforms to support targeted advertising options including Facebook (now terminated), Google, Twitter, AOL, eBay and MSN.[29]
Quantium	Quantium is a data consultancy that performs data analytics and builds artificial intelligence solutions. The company is 50% owned by Woolworths Group.[30] Clients include Woolworths, Facebook, NAB, David Jones, Suncorp and LendLease.[31]	**Facebook:** Until March 2018, Facebook used Quantium data to support ad targeting options within Facebook.[32] Facebook shut these types of partnerships down after the Cambridge Analytica scandal. **Woolworths Group:** Quantium provides data agency and scan interface services to Woolworths. This covers commercial reports and sales data to suppliers through the Woolworths web portal.[33] Woolworths Rewards outsources some of its data analysis to Quantium.[34] **NAB:** Quantium sources de-identified transaction data from NAB.[35] This data was use to support targeted advertising for Sportsbet.[36] **NewsCorp:** Quantium and NewsCorp have partnered to offer a News Connect product that combines NewsCorp's audience data with Quantium's database tracking shopping, travel and purchasing habits of 8 million Australians.[37]

27. Acxiom (2017) "2017 Annual Report" pp.10-11
28. Sloane, G. (28 March 2018) "Facebook Turns Off Ad Targeting Tool Based on Third-Party Data," AdAge, (https://adage.com/article/digital/facebook-turns-targeting-tool-based-party-data/312912/)
29. Acxiom (2017) "2017 Annual Report" p.10
30. Mitchell, S (4 October 2018) "Woolworths hands data sharing contracts to Quantium, Nielsen," Australian Financial Review, (https://www.afr.com/business/retail/woolworths-hands-data-sharing-contracts-to-quantium-nielsen-20181004-h16819)
31. Quantium website, accessed 3 April 2019, (https://www.quantium.com/)
32. Sloane, G. (28 March 2018) "Facebook Turns Off Ad Targeting Tool Based on Third-Party Data," AdAge, (https://adage.com/article/digital/facebook-turns-targeting-tool-based-party-data/312912/)
33. Mitchell, S. (4 October 2018) "Woolworths Hands Data Sharing Contracts to Quantium, Nielsen," Australian Financial Review (https://www.afr.com/business/retail/woolworths-hands-data-sharing-contracts-to-quantium-nielsen-20181004-h16819)
34. Chung, F. (13 July 2016) "The Price You're Paying for Loyalty," News.com.au (https://www.news.com.au/finance/business/retail/the-price-youre-paying-for-loyalty/news-story/c6c2316fc3faef5dc86cd917c0cf729e)
35. National Australia Bank (3 August 2017) "NAB Online Retail Sales Index: Indepth Report – June 2017" (https://business.nab.com.au/nab-online-retail-sales-index-indepth-report-june-2017-25397/)
36. Wallbank, P (29 March 2019) "Facebook shuts down third-party advertiser access in wake of Cambridge Analytica scandal" Mumbrella https://mumbrella.com.au/facebook-shuts-third-party-advertiser-access-wake-cambridge-analytica-scandal-508085
37. CMO Staff (31 July 2015) "News Corp Partners with Quantium and MCN to Launch New Digital Advertising Products," CMO, (https://www.cmo.com.au/article/580909/news-corp-partners-quantium-mcn-launch-new-digital-advertising-products/)

Experian	Experian collects and aggregates credit and demographic information. The 2016 Experian Annual Report claimed it had data on 918 million people and 107 million businesses, and marketing data on 700 million people.[38] Data suppliers include a range of consumer profiling and data aggregation businesses such as EightDragons, Acceleon, Illion, DSA, EgenticAu, Redial and UpsideDigital.[39]	**Facebook:** Until March 2018, Facebook used Experian data to support ad targeting options within Facebook.[40] Facebook shut these types of partnerships down after the Cambridge Analytica scandal. Partnerships are expansive and include notable technology companies such as SAP, Microsoft, and Oracle to enable validation, omni-channel marketing and audience profiling, data matching and enrichment, and consumer profiling and targeting capabilities for Experian customers.[41]
Epsilon	Epsilon states that they have a database of over 200 million customers. The company "enhances client customer data with Epsilon-held data to deliver customer insights".[42] Conversant, the digital arm of Epsilon, "holds customers data covering transactions, locations, and online behaviour across devices".[43] Epsilon collects data from public records, surveys, aggregator partners (e.g. product registrations and magazine subscriptions) and transactional data.[44]	**Facebook:** Until March 2018, Facebook used Epsilon data to support ad targeting options within Facebook.[45] Facebook shut these types of partnerships down after the Cambridge Analytica scandal. Epsilon's partnerships include Adobe, Oracle, IBM, SAP to support cross-channel campaigns, content and customer experiences.[46]

38. Experian (undated) "Discover Experian 2016" Annual Report (https://www.experianplc.com/media/2744/discover-experian-fy17.pdf)
39. Experian website (2019) "The Data We Obtain" (http://www.experian.com.au/consumer-information-portal/about-our-data)
40. Sloane, G. (28 March 2018) "Facebook Turns Off Ad Targeting Tool Based on Third-Party Data" AdAge, (https://adage.com/article/digital/facebook-turns-targeting-tool-based-party-data/312912/)
41. Experian (accessed 3 April 2019) "Partnerships and integrations" (https://www.edq.com/partners/)
42. Epsilon (2019) "Our Industry-Leading Experts are Ready to Grow Your Business" Epsilon website (https://emea.epsilon.com/data-driven-personalised-marketing-services#one)
43. Epsilon (2019) "What We Do Data" Epsilon website (https://emea.epsilon.com/data-driven-marketing-solutions/people-based-marketing-data-solution)
44. Adobe Audience Finder (2019) "Epsilon" (https://www.adobe-audience-finder.com/data_partner/epsilon/)
45. Sloane, G. (28 March 2018) "Facebook Turns Off Ad Targeting Tool Based on Third-Party Data" AdAge, (https://adage.com/article/digital/facebook-turns-targeting-tool-based-party-data/312912/)
46. Epsilon (2019) "Who We Are Our Partners" Epsilon website (https://apac.epsilon.com/people-based-marketing-solutions-epsilon/data-driven-marketing-solutions-partners)

Consequences for consumers

Data collection has become a part of the business infrastructure

Online business models are increasingly dependent on data collection. Large enterprises in all consumer facing markets rely upon this ongoing stream of data. Like many extractive industries that require more raw materials to expand, these data-driven businesses are reliant on the raw material of data in both their operation and growth.[47]

Personal data collection is increasingly inescapable

Data collection practices are pervasive and occur across multiple online and offline channels. Privacy protections, even when they are actively sought out by consumers, may not always be effective. For example, a Virtual Private Network (VPN) is often given as example of how consumers can protect their privacy online. In 2017, a Centre for Democracy and Technology investigation found that Hotspot Shield's VPN was sharing sensitive data – such as the name of wireless networks, MAC addresses, and device numbers – with third-party advertising networks – and not disclosing these practices to their users.[48] Avoiding services is also not necessarily the answer. For example,the ACCC found that Facebook was tracking the online activity of logged-in users, logged-out users, and individuals without a Facebook account.[49]

Data collection methods are opaque and the individual is transparent

Most consumers do not know the extent to which they are tracked. A 2018 New York Times analysis of apps collecting location information found that the explanations given to users are often incomplete or misleading. For example, an app may tell the user the information is collected to support the provision of traffic information, but the user is not told that the data will also be shared and sold.[50] Individuals' daily habits are now transparent to the parties and systems with access. In contrast, the practices of those parties and systems collecting the information are invisible to users. This results in a growing information and power imbalance between consumers and firms.

47. Manokha, I. (2018), "Surveillance: The DNA of Platform Capital—The Case of Cambridge Analytica Put into Perspective", Theory & Event, Volume 21, Number 4, October 2018, p. 895 (https://ora.ox.ac.uk/objects/uuid:15e74c10-225f-4bd7-b086-8e1fdb1b79e8)
48. De Mooy, M. (7 August 2017) "Hotspot Shield VPN's Privacy and Security Promises Contradict Practices. Centre for Democracy and Technology" CDT.org (https://cdt.org/blog/hotspot-shield-vpns-privacy-and-security-promises-contradict-practices/)
49. ACCC (December 2018) Digital Platforms Inquiry Preliminary Report, p.197 (https://www.accc.gov.au/system/files/ACCC%20Digital%20Platforms%20Inquiry%20-%20Preliminary%20Report.pdf)
50. Valentino-DeVries, J., Singer, N., Keller, M.H. and Krolik, A. (10 December 2018) "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," The New York Times (https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html)

Your life in data

As Australians move about their daily lives, online and offline services are tracking behaviour and movements through a range of technologies. Recent examples of consumer monitoring include:

App interactions

Many smartphone apps, across multiple sectors including travel, telecommunications and finance, are recording user interactions. Every interaction – such as a tap, or a swipe – is recorded and sent back to the app owners. For example, the Air Canada app wasn't properly securing the traffic that was sent back as part of the session replay and exposed passport numbers and credit card data.[51]

Surveillance cameras

Cameras were discovered embedded in the screens in Singapore Airline seats. Singapore Airlines has acknowledged that it is a camera but stated that they were disabled.[52]

Smart TVs

Samba TV is a software application that has deals with major television brands to install its software. When a consumer enables Samba TV, the software is able to track everything on the television screen on an almost second-by-second basis. The software is also able to identify other devices that share the TV's internet connection.[53]

Home alarm systems

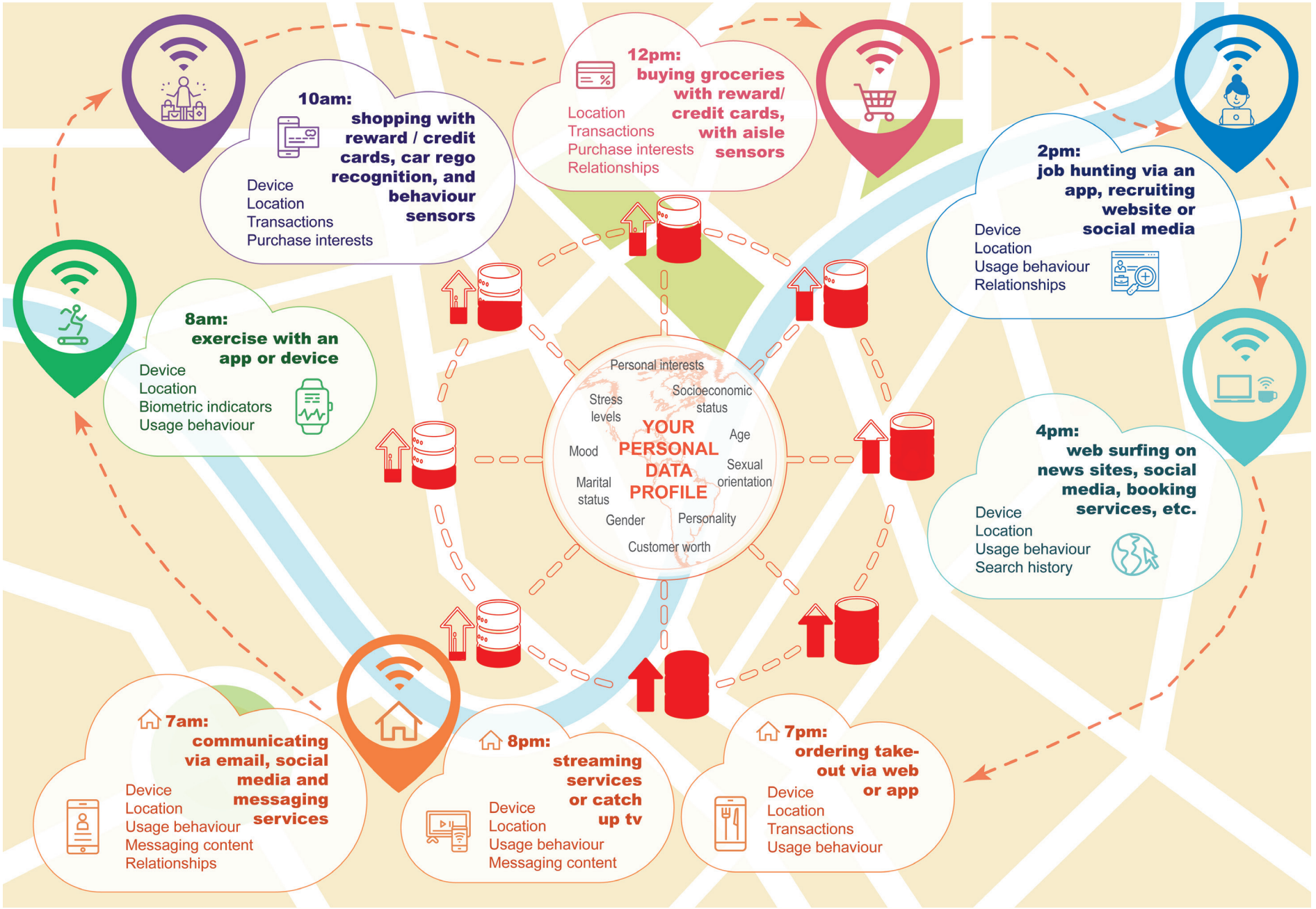
It recently emerged that the Nest Guard – an integral part of the Nest Secure home security and alarm system – had a previously undisclosed microphone. There was widespread concern as to why there was a secret microphone in a home alarm system and whether it had been in use. Google has stated that the omission of acknowledging the microphone was an error, it was not intended to be used until Google home assistant functionality was added to the Nest Guard and was not meant to be a secret.[54]

Personal information shared with Facebook

A recent Wall Street Journal investigation found that many apps were sharing personal information – such as intentions to become pregnant, heart rate monitoring, and real estate purchase interests – with Facebook, even if the user didn't have a Facebook account. Some of the information was shared with a unique advertising identifier that can be matched to an online consumer profile.[55]

The significant growth in the uptake of smart technologies by consumers only increases the scope for the collection of personal information, especially those located within the home – traditionally a place in which exchanges of the most personal and private aspects of our lives are made.

51. Whittaker, Z. (2019) "Many popular iPhone apps secretly record your screen without asking" TechCrunch (https://techcrunch.com/2019/02/06/iphone-session-replay-screenshots/)
52. Street, F. (3 March 2019) "Can airplane seat cameras spy on passengers?" CNN Travel https://edition.cnn.com/travel/article/airplane-seat-camera-intl/index.html
53. Maheshwari, S. (5 July 2018) "How Smart TVs in Millions of U.S. Homes Track More Than What's On Tonight" The New York Times (https://www.nytimes.com/2018/07/05/business/media/tv-viewer-tracking.html)
54. Osborne, C. (21 February 2019) "Google says 'hidden' microphone in Nest product never intended to be a secret" Zero Day in ZDNet (https://www.zdnet.com/article/google-says-secret-microphones-in-nest-home-products-an-error/)
55. Wall Street Journal investigation cited by Schechner, S. (22 February 2019) "You Give Apps Sensitive Personal Information. Then They Tell Facebook." Outline (https://www.outline.com/w5w5RP)



Christl, W. (June 2017) "Corporate Surveillance in Everyday Life" Cracked Labs. pp. 11 – 24 and pp.49-50 (https://crackedlabs.org/en/corporate-surveillance); Editorial Board (2 February 2019) "How Silicon Valley Puts the 'Con' in Consent," The New York Times, (https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html); Vlahos, J. (26 March 2019) "Smart talking: are our devices threatening our privacy?" The Guardian (https://www.theguardian.com/technology/2019/mar/26/smart-talking-are-our-devices-threatening-our-privacy); and Manwaring, K. (2017) "Will emerging technologies outpace consumer protection law? The case of digital consumer manipulation," Competition & Consumer Law Journal, 26, p.6

Common information collected within a 24hr period

Infographic 2 (p14) contains a simple demonstration of some of the typical data now being collected about consumers over the course of a single day. These examples can include a variety of indicators, such as:

- **Device:** This can include information on the hardware of the device, battery level, IP address, Unique ID and operating system.
- **Location:** Locations can be tracked in a variety of ways and with varying levels of granularity. Technologies that enable location tracking include GPS, Wi-Fi, and beacons.[56]
- **Usage behaviour:** A range of technologies, including cookies, web beacons and pixel tags, can be used to track a user's behaviour online, including interaction with websites and apps. This information may include time spent with a service, frequency of visits, and content interests.
- **Search history:** A list of all web searches performed, including the web pages visited and the paths taken.
- **Communications content:** The content of communications can be accessed or scanned by the service provider across a range of services. For example, Facebook Messenger content is scanned to check for rules violations. Messages are read if they were flagged by this process.[57] Voice recordings captured by the Amazon Echo speaker are reviewed by an Amazon team in order to improve the Alexa digital assistant software.[58]
- **Relationships:** For example, users' address books connected to a service, as well as interactions on social media platforms, can indicate familial and personal relationships.
- **Biometric indicators:** Types of measurements can include steps, distance travelled, active minutes, calories burned, heart rate, sleep duration and quality.[59]
- **Transactions:** This can include records of transaction on a particular website, or specific service, or transactions attached to a credit card or loyalty card. This data can provide insights into a wide range of factors such as health, income, addictions, political or charity donations.
- **Purchase interests:** This is a record of what products or services a user has shown interest in or purchased.

Taken combined, this vast amount of data enables firms to develop increasingly detailed profiles of individuals. The processing of this data can then lead to inferred personal information such as: socioeconomic status, sexual orientation, political views, personality, mood, stress levels, health, personal interests, consumer worth or value or relationship status.

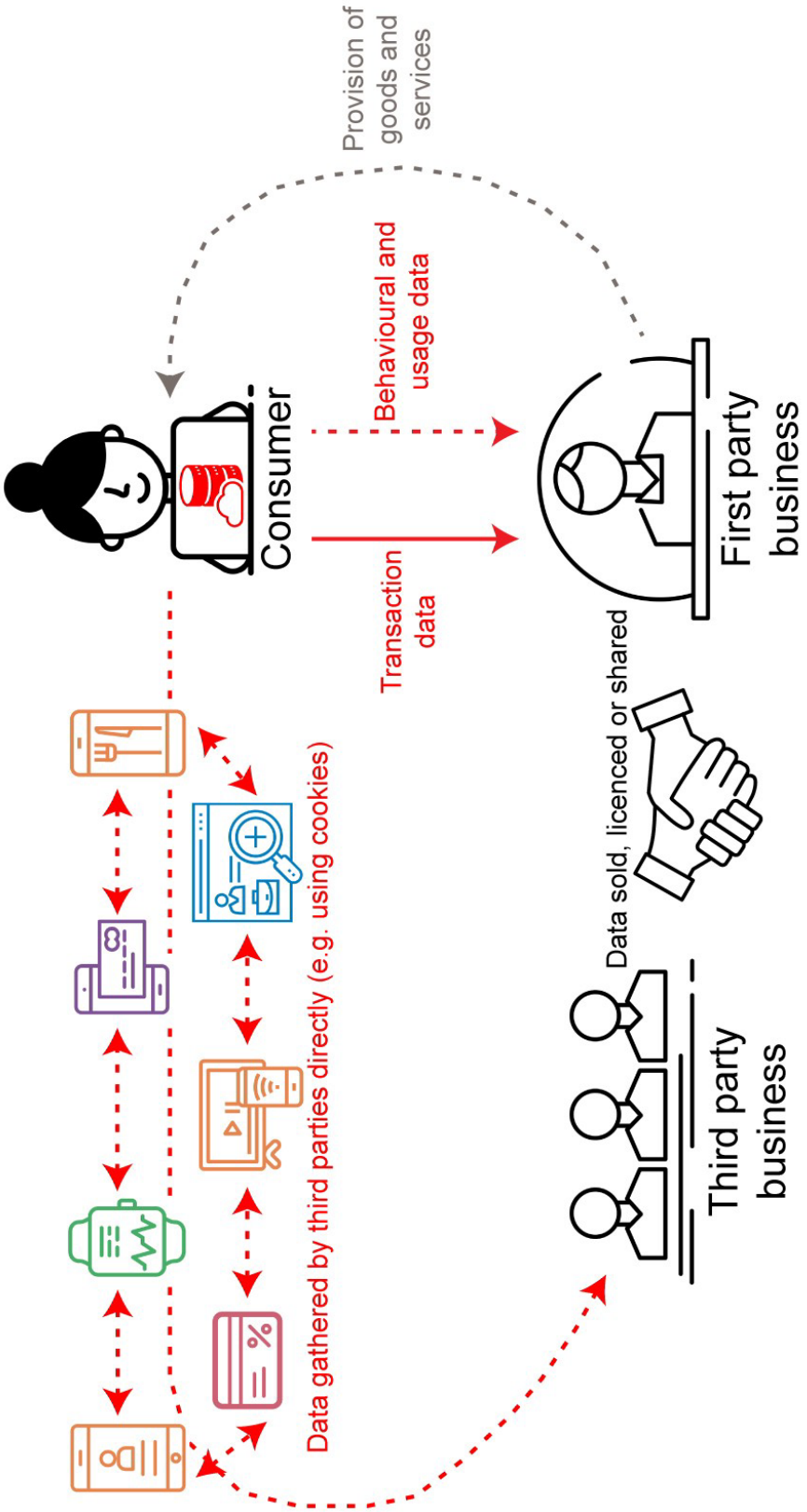
Taken combined, this vast amount of data enables firms to develop increasingly detailed profiles of individuals. The processing of this data can then lead to inferred personal information such as: socioeconomic status, sexual orientation, political views, personality, mood, stress levels, health, personal interests, consumer worth or value or relationship status.

The information and inferences made from this information is stored in various profiles that can be combined in different contexts to support predictive analytics and programmatic advertising. The analysis may be used to not only advertise, but also influence consumer behaviour. This is discussed in more detail in the chapter on harms (p34).

Infographic 3 (p16) shows how this data is often shared and reshared through a web of relationships between companies and data brokers.

56. Nguyen P. and Solomon L. (2018) Consumer Data and the Digital Economy, Melbourne: Consumer Policy Research Centre, pp.11 (http://cprc.org.au/2018/07/15/report-consumer-data-digital-economy/)
57. Ovide, S. (6 April 2018) "Private Messages Aren't Exactly Private at Facebook" Bloomberg (https://www.bloomberg.com/opinion/articles/2018-04-05/facebook-private-messages-aren-t-exactly-private)
58. Day, M, Turner, G and Drozdiak, N (11 April 2019) "Amazon workers are listening to what you tell Alexa" Bloomberg (https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio)
59. Fitbit website (2019) "Versa" (https://www.fitbit.com/au/versa)

Infographic 3: Data Sharing Cycle



Consumer perspectives

CPRC conducted consumer research in two phases. Firstly, we hit the streets of Melbourne to talk directly with consumers about their experiences engaging companies and their attitudes towards privacy.

Secondly, CPRC engaged Greater Than X to explore data collection and the consumer experience as they go about their daily lives. Greater Than X designed a qualitative technical experiment that used a hybrid methodology of contextual inquiry and usability to test two hypotheses:

1. When presented with legal agreements in an online transaction, consumers have limited choice.
2. When presented with the extent and details of data collection and processing, consumers are uncomfortable and will be more likely to take a proactive stance to protect their privacy.

Attitudes and behaviours of consumers in relation to privacy

CPRC conducted brief interviews with people on the streets of Melbourne in March and April 2019, with conversations covering attitudes towards privacy, data collection, the utility of privacy policies and consumer control over data (see pages 18 and 19). None of the interviewees read privacy policies and often expressed that, while they found these documents hard to understand, they felt guilty for not reading the policies.

Interviewees felt, despite finding privacy policies hard to understand, that they had control over the information collected about them and that it was their responsibility to protect their privacy. Multiple interviewees commented that they restricted the number of friends connected to their social media profiles, that they were conservative about the information they disclosed on the internet, and that they only used what they perceived to be 'reputable' online services. None of the participants considered the data they produced through daily access to the internet.

This acceptance of responsibility only changed when the conversation moved to data collection and use beyond targeted advertising. CPRC presented the example of US insurance companies experimenting with using social media information to adjust insurance costs.[60] As the discussion turned to possibility of errors or judgements about ongoing behaviour made on the basis of one photo, participants grew noticeably more unsure and uncomfortable about the use of their data.

60. Heller, N. (26 February 2019) "Why the Life-Insurance Industry Wants to Creep on Your Instagram" New Yorker (https://www.newyorker.com/culture/cultural-comment/why-the-life-insurance-industry-wants-to-creep-on-your-instagram)

Interviews with consumers - Melbourne - March/April 2019
Do you read privacy policies?

"[I] just click it. It's pretty bad I think."

- Participant 1

"No. I do sometimes. I have read the Facebook ones when they change, but then you know they change again and you go, oh I just can't be bothered reading it again."

- Participant 10

"I might have a skim if it's there… if it's one of those ones you have to physically scroll through to get through to the acceptance section I would but if it's something that you have to open separately to approve I would never."

- Participant 8

"maybe a skim at most... too much technical information... the wall is too high."

- Participant 6

"No…it's a lot of effort… you have to go in and read a lot material…and that can take time and when you just want to get in and get your transaction done and your tickets bought you just tick the box and move on and hope for the best. That's what I do."

- Participant 4

Interviews with consumers - Melbourne - March/April 2019
Can people control their online privacy?

"I don't post anything on there that I really wouldn't be comfortable with a job or a friend or stranger seeing."
- Participant 8

"[Social media] can be very private if you want to…I think it's a person's choice to show this information."
- Participant 5

"…people post things they definitely shouldn't post"
- Participant 1

"I think [I have control]…with the privacy settings that I've got…and I control my friendship groups."
- Participant 10

Interviews with consumers - Melbourne - March/April 2019
Thoughts on insurers using social media to adjust premiums?

"People's social media... [is] not always accurate. Probably not necessarily an indication of...their true self."
- Participant 6

"I wouldn't like that."
- Participant 9

"The intent is not that your life would be evaluated by an insurance company, and that might change how you use it"
- Participant 10

I guess I've made assumptions that a big conglomerate wouldn't look at me.
- Participant 8

"It doesn't make any sense."
- Participant 5

Experiment design

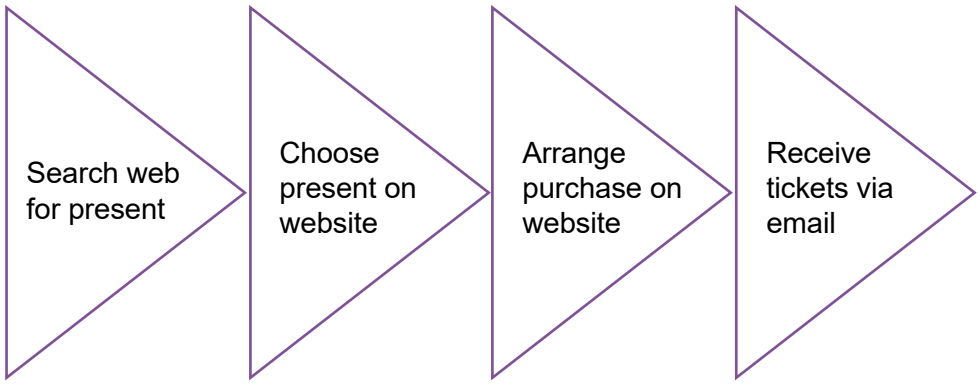
Greater Than X conducted a qualitative experiment that tested consumer perspectives and reactions as they went through the process of searching for a Valentine's Day present online, purchased a romantic cruise, paid for the order and received the tickets via email.

The participants were not performing a live internet search. Greater Than X created a clickable prototype that mimicked the experience of searching, purchasing and paying online. The experience of the search, purchase, and payment process was designed to reflect the common practices used in data collection and processing. The actual privacy policies and terms and conditions were used for the following services mimicked in the experiment: PayPal, Apple and Google. The cruise website's privacy policy and terms and conditions were modified versions of actual agreements offering similar services.

Appendix 1 (p60) outlines the theory underpinning the choice of experiment and explains why this type of research is the most suitable for explore the consumer experience with data collection.

The process followed by the participants is shown in Infographic 4 (below).

Infographic 4: Online Search and Purchase of a Valentine's Day Present



There were six participants, all female, aged between 28 and 40 years old, and working part-time.

The research sessions were conducted using a laptop connected to a large screen display to observe participant interactions. The screens shown were those usually seen on mobile phone screens. The participants' behaviour and reactions during the research sessions were observed and recorded by a note taker.

As the users progressed through the search, purchase, and payment process, Greater Than X observed the participants' responses, observed behaviour, key words, emergent themes, and inferred behavioural state.

A full methodology, including the interview script, is provided in Appendix 1 (p60).

Overall insights

Experiment stage: Privacy policies

Participants were asked to approve terms and conditions and updated privacy policies several times during the experiment, including when they visited the website to view the present and during the purchase process.

Insight: Consumers have limited choice

All participants attempted to accept the legal agreements without reading the documents. On average, the participants took no more than two seconds to either select “Yes, I Accept” or close the notice. The total time to read all four legal agreements presented during this experiment would take more than three hours on average. When directed to read the primary party’s privacy policy, participants averaged four minutes after which they indicated they wanted to stop reading.

Participant 1 stated that while she knows “there is very little choice in purchasing things online,” she feels that she has to do it. Session 5’s participant noted how “all companies have it,” and if she wanted a product, she needed to agree to the company’s privacy policy. She further explained her decision as there being a choice to opt out, but the choice being unrealistic, stating “I do have a choice, but to get the deal I don't have a choice.”

Insight: Legal agreements need to be simplified

Participants agreed that legal agreements need to be simplified. All participants skimmed through the primary privacy policy in less than four minutes. When questioned about their understanding all participants suggested an improvement is needed to the readability and length of the legal agreements presented.

Participant 1 asserted that “a condensed version should be available”, despite dismissing it and stating “it wouldn't happen”. Participant 2 commented that, “for the simple person, this will be a complete mumbo jumbo” and a “condensed version should be available”. Participant 3 questioned “I don't know why it [privacy policy] needs to be so long”. Participant 4 described the policy as being “in words that we cannot even think in. It doesn't even make sense in relevance to the product”, stating that the policy needs to be in “simple” words.

Apprehension towards legal agreements was most clear in Participant 5, who scoffed at the researcher.s suggestion to read the privacy policy, saying “well you need to have a master’s degree to understand this.” She went onto state that she feels that “they write it purposely so that normal people cannot understand it” and that consumers should be able to “skim through” a policy that highlights what “you need to know as a customer”.

Insight: Disempowerment leads to apathy

Participants described the four privacy policies and practices shown in the experiment as “standard” despite the differences between the four documents, indicating apathetic behaviour arising from limited choice and understanding.

Participant 3 explained that she is aware that the data “is just out there”, but even if she went to brick-and-mortar shops “they are already collecting data on me. That’s just the way shopping works these days”. The inescapability of data collection has led to the disempowerment of consumers, making them feel apathetic towards data collection and processing. Participant 6 showed this apathy, commenting that “I feel like it's standard. You read it everywhere. so yeah... okay. Let me just purchase what I came here for.”

All participants attempted to accept the legal agreements without reading the documents. On average, the participants took no more than two seconds to either select “Yes, I Accept” or close the notice.

Experiment stage: Disclosing personal information

Participants were asked to give personal information multiple times during the purchase and payment processes. Participants were also shown targeted advertisements based on their search history of "Valentine's Day'" at the start of the experiment.

Insight: Apathy leads to indifference

Participants' sense of disempowerment led to a psychological removal of current data practices from critical judgement.

Behavioural patterns of the participants paralleled each other when addressing their indifference towards privacy. Participant 3 expressed her lack of concern for her "details", stating "I am not too bothered, to tell you the truth" as she laughed, swinging her chair away from the screen. Participant 6 also laughed and shrugged as she went onto state "I mean what are you gonna do? Not leave the house?" addressing her views on current data collection methods. She went on to dismiss explanation of current data processes with "yeah", "fine", "whatever" and "cool", cutting in before the explanation was over. When making some final comments at the end of the session, Participant 1 said "I brush it off I guess. It just needs to be done... Well it doesn't need to be, but everyone wants things to be as convenient as possible".

Insight: Consumers empathise with companies

Empathy emerged across all six sessions as the participants' tried to explain their reasoning of companies' data collection and processing activities.

Participant 6 stated, "protecting the company is protecting me". Participant 2 repeated the expression "fair enough", stating that she feels that the company needs "all my personal information" to complete her transaction.

The participants also put the responsibility on themselves, not the companies. Participant 5 said if she signs up to a service or product without reading their privacy policies in full, the company "fulfilled their duties" and it will be her "own fault". Participant 2 also noted how she doesn't "want to blame other people" and that "at the end of the day, the company needs to do this to cover for what may happen".

Participant 1 said "I brush it off I guess. It just needs to be done... Well it doesn't need to be, but everyone wants things to be as convenient as possible".

Experiment stage: Debrief

After the experiment researchers discussed the data collection landscape. Participants were provided with verbal explanation of how personal information during this one process of searching for a Valentine's Day present can be shared with over 300 parties, funnelled through data brokers and used to connect that information with the participant's online profile. Visual drawings on paper were used to support explanation and participant comprehension.

Insight: Learning leads to dismay, then proactiveness

During the debrief participants' behaviour indicated apparent discomfort. Participant 1 commented that "It's terrifying when you think really deeply into it…" Participants 3 and 5 both commented on how scary the information was. 5 of the 6 participants crossed their legs or arms, with Participant 5 crouching to coil into herself. The other 5 participants were sitting straight up on their chair as information was given, with various gestures of discomfort such as looking away from the interviewer, hands around the neck and clenching of fist.

The body language that indicated dismay was soon followed by proactive questioning about alternatives to their current habits. Participant 3 asked questions throughout the session on various topics such as which sites are safer and the meaning of certain privacy policies. At each mention of data collection practices her body language coiled into herself, her arms wrapping around her upper body. This body language became more open post-debriefing, as she expressed interest for the sticker over the camera of the laptop used during the experiment, stating "I will put a sticker on my camera now".

Participant 4 shared buying an item from Google and then beginning to see ads for similar products on Facebook. Her dismay was clear as she explained how "no one else knows this, not even my friends" in a high-pitched voice, crossing her arms to say "but somehow Facebook knows". This enthusiasm towards privacy was clear as she re-evaluated sharing her purchase confirmation with her calendar application, commenting "now I am thinking how many companies have my information".

Participant 1 commented that "It's terrifying when you think really deeply into it…" Participants 3 and 5 both commented on how scary the information was.

Privacy policies

Online and offline services provide privacy policies, terms and conditions, cookie statements and other documents to explain their data collection, sharing and use practices, and to provide a contractual basis for user consent to the terms and conditions of using the service.

A number of concerns have been highlighted around the content and process of accepting privacy policies and terms and conditions of service, including:

Length

The New York Times found that the average person would need to spend 76 days to read all the digital privacy policies that they have agreed to in that year.[61]

Complexity

Privacy policies also tend to be difficult to understand. One study found that the average readability of the privacy policies of the top 500 websites in the US was around the same level as academic journals.[62]

Take-it-leave it terms

The ACCC analysis in its Digital Platforms Inquiry highlighted the prevalence of "click-wrap" agreements. This refers to the common practice of nudging consumers to agree to privacy policies on take-it or leave-it terms without fully engaging in the terms and policies of use.[63] Concerns have been raised that these "click-wrap" agreements are nudging people to automatically accept any digital contract for service access without thinking. Creating a frictionless process for acceptance – phrased as techno-social engineering – causes contractual arrangements to be automatic and ubiquitous. Researchers have flagged that these sorts of agreements ultimately erode consumer autonomy.[64]

Unclear consequences of changes to privacy controls

Many privacy policies allow consumers to make changes to privacy controls but also make unspecified warnings of negative consequences should they choose to do so. Zuboff, in analysing the Nest ecosystem, found that the purchase on one thermostat would require the review of nearly a thousand contracts. Customers refusing to agree to Nest's terms of service are warned that the operations and security of the thermostat will be deeply compromised.[65]

Difficulty for consumers to control their privacy settings

A study of the parent organisations of the top ten advertising and tracking services, including Alphabet and Facebook, found that their privacy policies did not allow users to opt-out completely of being tracked or sharing data with organisations.[66] Another study found that the overwhelming amount of granular choices available on the Google privacy dashboard had the effect of discouraging users to take control of the settings or delete data.[67] An Associated Press investigation in 2018 found that many Google services still stored location information even if the privacy settings were set to prevent Google from tracking locations.[68]

The New York Times found that the average person would need to spend 76 days to read all the digital privacy policies that they have agreed to in that year.[61]

61. Editorial Board (2 February 2019) "How Silicon Valley Puts the 'Con' in Consent," The New York Times, (https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html)
62. Benoliel, U. Becher, S. I. (11 January 2019) "The Duty to Read the Unreadable" 60 Boston College Law Review (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3313837)
63. ACCC (December 2018) Digital Platforms Inquiry Preliminary Report, p.197 (https://www.accc.gov.au/system/files/ACCC%20Digital%20Platforms%20Inquiry%20-%20Preliminary%20Report.pdf)
64. Frischmann, B. (19 February 2019) "Electronic Contracts and the Illusion of Consent" Scientific American (https://blogs.scientificamerican.com/observations/electronic-contracts-and-the-illusion-of-consent/)
65. Zuboff, S. (2019) The Age of Surveillance Capitalism, New York: Hatchette Book Group, p.7
66. Razaghpanah, A. (18-21 February 2018) "Apps, Trackers, Privacy and Regulators. A Global Study of the Mobile Tracking Ecosystem" Network and Distributed Systems Security (NDSS) Symposium, p.9
67. Norwegian Consumer Council (27 June 2018) Deceived by Design, p.39 (https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf)
68. Whigham, N. and Associated Press (14 August 2018) "Google will keep tracking your every movement, like it or not" News.com.au (https://www.news.com.au/technology/gadgets/mobile-phones/google-will-keep-tracking-your-every-movement-like-it-or-not/news-story/7f6daa18cbe444cc11e2b1360e63f857)

Case studies of eight privacy policies

CPRC has chosen eight privacy policies including associated cookies policies, terms of use, and collective statements to examine in more detail based on widespread concerns around the length and complexity of privacy policies and the difficulty for consumers to make informed decisions based on these documents. The eight policies were chosen to cover as wide a range of activities and business types as possible. This includes a mix of online and bricks-and-mortar businesses, Australian and international businesses, as well a range of different activities. The services were also chosen for how commonly these activities are undertaken in the daily lives of Australian consumers. Table 2 outlines the eight policies, the documents analysed, the reading time and education level required by consumers to comprehend the information provided.

Table 2: Examples of Data Sharing Arrangements

Policy	Business type	Geographical coverage	Documents analysed	Hemingway App Analysis		Date of Document	Date accessed
				Education level for document	Reading time for document		
Visa	Credit card	Australia	Global privacy notice Additional privacy notice for Australia Visa Checkout Privacy Policy*	12	14 min, 7 sec	23/05/2018 2019 23/05/2018	24/05/2019 24/05/2019 24/05/2019
Woolworths Reward	Super market loyalty program	Australia	Woolworths Rewards Collection Notice Woolworths Group Privacy Policy* Woolworths Cookie Statement	10	8 min, 2 sec	06/06/2018 01/2018 2019	24/05/2019 24/05/2019 24/05/2019
Westfield	Shopping centre	Australia	Scentre Group Privacy Policy	12	30 min, 50 sec	01/08/2018	13/02/2019
9Now	Catch-up TV	Australia	Nine Entertainment Co. Privacy Policy* nine.com.au Terms and Conditions	13	12 min, 3 sec	Undated 26/09/2017	13/02/2019 13/02/2019
LinkedIn	Networking site	Global	LinkedIn Privacy Policy* LinkedIn Cookie Policy	11	23 min, 56 sec	08/05/2018 08/05/2018	13/02/2019 13/02/2019
MindBody Online	App for wellbeing appointments	Multiple countries	MindBody Privacy Policy* MindBody Cookies Policy	12	24 min, 43 sec	31/12/2018 25/04/2018	13/02/2019 13/02/2019
iSelect	Comparison website	Australia	iSelect Privacy Policy*	11	11 min, 57 sec	01/2019	13/02/2019
Snapchat	Social media	Global	Snapchat Privacy Policy* Snapchat Terms of Service Snapchat Cookie Policy	10	15 min, 45 sec	01/10/2018 18/02/2019 15/01/2019	13/02/2019 24/05/2019 13/02/2019

*Note: * denotes the document used for the Hemingway app analysis*

Note: Date of privacy policy documents given to denote the version analysed. Policy document content may change with subsequent updates.

Working again with our partner Greater Than X, our analysis has focused on the following aspects of privacy policies:

- Readability and consumer comprehension
- Definition of personal information
- Description of third-party data sharing
- Location data
- Consumer control

Readability and consumer comprehension

All privacy policies required a significant commitment of time and at least a Year 10 (US grade level) educational level to comprehend. The reading time and education level of each privacy policy shown in Table 2 was analysed using the Hemingway Editor App.[69] This app assesses the "readability" of a written document and can assess the reading level (by US grade level) required for a consumer to understand the content.

All privacy policies required a reading level of Grade 10 or higher, with one requiring a university level of education. In 2008, Australian Bureau of Statistics research found that forty-six percent of Australian adults aged 16 to 70 years old lacked the document literacy to perform simple workplace skills,[70] suggesting that a substantial proportion of the population may have difficulty understanding these privacy policies.

Seven of the eight privacy policies analysed would take over 10 minutes to read. We note that most privacy policies also connected to cookie policies, terms of service and other documents that would add additional minutes and complexity to the reading process. It is unlikely that the majority of consumers are reading all of these materials before accessing a service. Greater Than X's qualitative consumer experiment showed that participants generally wanted to stop reading after four minutes.[71]

69. Hemingway Editor (2015) "Help" (http://www.hemingwayapp.com/help.html)
70. Australian Bureau of Statistics (2008) "1367.2 – State and Regional Indicators, Victoria, June 2008" (http://www.abs.gov.au/AUSSTATS/abs@.nsf/featurearticlesbyCatalogue/8121E0B13EA1139FCA25750700146C83?OpenDocument#Link5) cited in Vocational Literacy (undated) "ABS Research: 46% of Australians Adults Aged 16-70 are Illiterate" (http://vocationalliteracy.com.au/research-into-adult-literacy-in-australia/)
71. Refer to Your Life in Data (p13).

Vague descriptions of information collected

The privacy policies examined are generally quite vague on what types of information may be collected through these policies. General, non-exhaustive examples of what information "may" be collected are used in many of the policies rather than specific definitions of what is meant by personal information. The vague terms and examples used allow the service provider a wide scope in which to collect additional information that may be associated with a user's profile.

The Global Visa privacy notice defines personal information as, "…any information that we can use to identify, locate or contact you. It also includes other information that may be associated with your Personal Information, such as demographic data".[72] The notice does not provide exhaustive examples of "other information", and includes a fairly broad statement that service usage and preference information may be collected as well as "similar information that can help us understand you and offer you personalised content and offers", such as enhanced demographic data sourced from the census.[73]

This lack of specificity or clarity on data collection inhibits consumers' ability to understand what information they are providing when they take up a service or to provide informed consent on that basis. There is a lack of specificity about the size and scale of the information collected. For example, the Woolworths Rewards collection statement notes that it collects transaction information both when the Rewards card is scanned, and when the user's payment card is scanned as it is matched to the Rewards account.[74] This results in a much larger data collection that extends beyond Woolworths Rewards related purchases. The emergence of services like Cardlytics, who uses anonymised transaction data to identify marketing opportunities,[75] shows the value of monitoring transaction data. Consumers are unlikely to realise the value of the information they are providing when they agree to these privacy policies.

This lack of specificity or clarity on data collection inhibits consumers' ability to understand what information they are providing when they take up a service or to provide informed consent on that basis.

Opaque description of third-party sharing

The eight organisations disclosed sharing arrangements with third parties, including parent companies or subsidiaries and entities described as affiliates or "trusted partners". This can be in the form of sourcing additional information about their own users to create enhanced consumer profiles or through sharing anonymised datasets with other parties. These data sharing relationships are described in non-specific terms. The information provided on what data is shared and why is often vague and unclear.

72. Visa Global Privacy Notice (23 May 2018) "1. What Personal Information is Collected" (https://www.visa.com.au/legal/global-privacy-notice.html) (accessed 24 May 2019)
73. Visa Global Privacy Notice (23 May 2018) "1. What Personal Information is Collected" (https://www.visa.com.au/legal/global-privacy-notice.html) (accessed 24 May 2019)
74. Woolworths Rewards Collection Statement (6 June 2018) "Collection from Members" and "Collection from Others" (https://www.woolworthsrewards.com.au/privacy.html) (accessed 24 May 2019)
75. Cardlytics (2019) "About us" (https://www.cardlytics.com/about-us/our-story/) (accessed 24 May 2019)

Table 3: Examples of Data Relationships

Privacy policy examples	Examples of data relationships
Visa	**Oracle:** Oracle Data Cloud's digital advertising and cross-device connection data is used in conjunction with aggregated purchase data from Visa Advertising Solutions to measure consumer responses to advertising campaigns across marketing channels.[76] **PayPal:** Visa and PayPal have announced a partnership, part of which includes an agreement that some data sharing about Visa-funded transactions will occur between Visa and PayPal for the purposes of fraud prevention.[77]
Woolworths Rewards (Woolworths Group)	**Quantium:** Woolworths Group shares sales data with Quantium. Woolworth Rewards shares data with Woolworths suppliers via Quantium.[78]
9Now	**Microsoft:** Nine Entertainment Co. attaches behavioural and device data (including that sourced from 9Now) to Microsoft user accounts.[79] **Experian**: Nine Entertainment Co. checks the integrity of its data (including 9Now data) with Experian.[80]
LinkedIn	**Microsoft:** Users connecting their LinkedIn and Microsoft accounts allow Microsoft to access, store and use profile, interests, subscriptions and connections data.[81]

A number of the policies mention sourcing customer information from third parties to create enhanced user profiles. Snapchat provides examples of the instances in which they might receive information about the user from other users, affiliates (defined as Bitstrips Inc., Zenly SAS and Placed Inc.) and third parties. It is unclear whether these examples are the main instances or in what other contexts Snapchat might receive information.[82] MindBody states that it collects information from "public databases, strategic and joint marketing partners, social media pages and platforms, people with whom you are friends or otherwise connected on social media platforms, as well as from other third parties". Users who sign in with their social media accounts may have elements of their social media accounts shared with MindBody, including profile information of the user and the user's friends.[83] These statements in the privacy policies suggest that protecting one's own privacy is not sufficient when an individual's information may be shared via other means, be their contact lists or social media profiles.

76. Business Wire (27 September 2018) "Visa and Oracle Introduce New Tools to Help Improve Digital Ad Performance" Business Wire (https://www.businesswire.com/news/home/20160927005676/en/Visa-Oracle-Introduce-New-Tools-Improve-Digital)
77. Guess, M. (22 July 2016) "PayPal Will Share Data, Plug Visa in Exchance for Wider Terminal Acceptance" ArsTechnica (https://arstechnica.com/information-technology/2016/07/paypal-will-share-data-plug-visa-in-exchange-for-wider-terminal-acceptance/)
78. Woolworths (4 October 2018) "Announcement from Peter and Paul" (http://www.wowlink.com.au/cmgt/wcm/connect/345dfe80473b4826a32ca35fa1287528/Update+on+Woolworths+Data+Sharing+RFP.pdf?MOD=AJPERES)
79. Nine (2018) "Data & Targeting" (https://www.nineentertainmentco.com.au/brand-data) (accessed 24 May 2019)
80. Nine (2018) "Data & Targeting" (https://www.nineentertainmentco.com.au/brand-data) (accessed 24 May 2019)
81. LinkedIn (2019) "LinkedIn in Microsoft Applications with Your Personal Account" (https://www.linkedin.com/help/linkedin/answer/84711/linkedin-in-microsoft-applications-with-your-personal-account?lang=en) (accessed 27 May 2019)
82. Snapchat privacy policy (1 October 2018) "Information We Collect from Third Parties" (https://www.snap.com/en-US/privacy/privacy-policy/) (accessed 13 May 2019)
83. MindBody Privacy Policy (31 December 2018) "How We Collect Information" (https://www.mindbodyonline.com/privacy-policy) (accessed 13 February 2019)

Case study: Enhanced profiling with Woolworths Rewards

Woolworths Rewards's collection notice states that, "at times, we [Woolworths Rewards] combine different sets of data to add to the personal information we hold".[84] This combined information would create an enhanced profile of their members. For example, the member's credit card that is used in conjunction with the Rewards card is tracked whether or not the Rewards cards is used in that transaction.[85] Woolworths Rewards states that it also collects personal information about members from other persons and entities. These entities are not defined, but examples stated in the collection notice include insurers, third party data providers, and delivery service companies.

The collection notice states that the information is collected for the purposes of customer analytics (on an aggregated or anonymised basis), direct marketing, tailored advertising, products and market research, business improvement and other operational purposes. However there is a more general sentence included in this section on why personal information is collected, stating that information is also collected "for other purposes which are within Woolworths Rewards Members' reasonable expectations or permitted by law".[86] This is a very broad sentence and it is unclear what types of activities would be included within the meaning of this statement.

These data collection practices allow Woolworths Rewards a far more detailed profile of the consumer than may be expected when a member initially signs up. Woolworths is not only collecting rewards-based transaction details but appears to be collecting a whole other range of information that is not specifically defined in the collection notice and which could have important implications for the inferences made about a consumer. For example, delivery service company information could include the amount and frequency of food deliveries ordered by a user. This information, combined with insurance information, could in some contexts have the capability to infer health risks. While CPRC is not suggesting this is precisely what is occurring, the lack of specificity in the collection notice makes it difficult to conclude how different datasets are currently being used. The combining and sharing of consumer data to develop or infer customer attributes and risks is discussed further in the chapter on harms (p34).

Over half of the privacy policies also disclose the sharing of data with other parties on an anonymised, aggregated or de-identified basis. For example, the Woolworths Rewards collection notice states that it shares "aggregated and anonymised information to our trusted partners (including our suppliers) about Woolworths Rewards Members' attributes, behaviours and preferences to enable them to market products and services that most likely to interest you based on those attributes, behaviours and preferences".[87]

Visa notes that it will "generate anonymised and aggregated datasets, which can be used for modelling, reporting and analytics".[88] None of the privacy policies specify all of the companies receiving the data or the intended purposes of these arrangements. Page 31 outlines some of the pitfalls on relying on de-identification processes to protect consumer anonymity.

84. Woolworths Rewards Privacy Policy (6 June 2018) "Collection from Others" (https://www.woolworthsrewards.com.au/privacy.html) (accessed 24 May 2019)
85. Woolworths Rewards Privacy Policy (6 June 2018) "Collection from Members" and "Collection from Others" (https://www.woolworthsrewards.com.au/privacy.html) (accessed 24 May 2019)
86. Woolworths Rewards Privacy Policy (6 June 2018) "Collection Purposes" (https://www.woolworthsrewards.com.au/privacy.html) (accessed 24 May 2019)
87. Woolworths Rewards Privacy Policy (6 June 2018) "Disclosure to Others" (https://www.woolworthsrewards.com.au/privacy.html) (accessed 24 May 2019)
88. Visa Global Privacy Notice (23 May 2018) "3. How We Use Personal Information" (https://www.visa.com.au/legal/global-privacy-notice.html) (accessed 13 February 2019)

The risks of relying on de-identified data

When describing the data collection process, it is important to note that the collected and then amalgamated data is de-identified or anonymised. Australia, as do most jurisdictions, has protections around the collection, sharing and use of personal data. De-identifying information turns personal information into non-personal information that can be shared, commonly through hashing or assigning a unique identifier to a user.[89]

However, research has demonstrated that de-identified data – such as telephone metadata, transactional history, and social network connections – can be re-identified.[90] For example, anonymised mobile phone location data can be re-identified. Academic research found when the location of a person is updated hourly, only four spatio-temporal data points are necessary to identify 95% of individuals. Two spatio-temporal data points would identify 50% of individuals.[91] Similarly, 2017 research from Melbourne University outlined the relative ease through which data from the Australian Medicare benefits Scheme (MBS) and the Pharmaceutical Benefits Scheme (PBS) that was released publicly in 2016 could be re-identified through linking known personal information, such as year of birth and known medical procedures.[92]

Consequently, the data lakes of aggregated, anonymised, or de-identified data sitting on servers around the world still carry substantial risk of re-identification.

Case Study: Nine Entertainment Co. and 9Now data

The Nine Entertainment Co. privacy policy states to consumers that personal information from third party sources and platforms – such as social media, online marketing companies, Microsoft Products – may be used to supplement a user's profile. Users of the service that connect using their social network profile are consenting to 9Now accessing and using certain information from that social network profile. It is not disclosed what that information might be. The Nine Entertainment Co. privacy policy states: "You acknowledge and agree that information including your personal information may be shared with the Nine Entertainment Co. group of companies and provided to third parties and used by those organisations for any of the purposes disclosed in this privacy policy." Users are not able to optout of this data collection.[93]

However, Microsoft and Nine Entertainment Co. in advertising their partnership and rich data assets to potential advertisers state that Nine has: 300 touchpoints including search, mobile, gaming, email, online shopping and more – allowing them to build a "360 view of a consumer, modelling end user behaviour and cross-device consumer behaviour". Further, the partnership enables them to "see beyond buckets of intention behaviour to more complex path to purchase behaviour for specific brands". Audience/Match Sync service enables "matching or syncing against the largest scale of registered users in Australia allows advertisers to find their offline email databases or DMP segments across the entire breadth of our digital assets – starting intelligent dialogue, rewarding customers for their loyalty, designing upsell and cross-sell strategies, and finding new "lookalike" customers".[94] These differing perspectives on the same data collection and sharing process presented to consumers – as compared to potential business partners and advertisers – highlights the potential information gap and misunderstanding even for highly engaged, committed consumers attempting to read privacy policies in full.

These examples show that sharing data with, and sourcing data from, third parties is a widespread practice. The methods and purposes of these practices are fairly opaque even for close readers of privacy policies. In many cases, the consumer has limited ability to opt-out of these arrangements.

89. ACCC (2018) Digital Platforms Inquiry: Preliminary Report, p.188 (https://www.accc.gov.au/system/files/ACCC%20Digital%20Platforms%20Inquiry%20-%20Preliminary%20Report.pdf)
90. Research quoted in ibid.
91. de Montjoye, Y. A., Hidalgo, C.A., Verleysen, M. and Blondel, V.D. (25 March 2013) "Unique in the Crowd: The Privacy Bounds of Human Mobility," Scientific Reports 3, Article Number: 1376 (https://www.nature.com/articles/srep01376)
92. Culnane, C Rubinstein, B I P and Teague V. (December 2017) "Health Data in an Open World" (https://arxiv.org/ftp/arxiv/papers/1712/1712.05627.pdf)
93. Nine Entertainment Co. Privacy Policy (Undated) "Information we collect from other sources" (https://login.nine.com.au/privacy?client_id=9nowweb) (accessed 13 February 2019)
94. Nine Entertainment Co. (21 March 2019) "Data & Targeting" (https://www.nineentertainmentco.com.au/brand-data) (accessed 24 May 2019)

Location data

Many of the privacy policies collected location data with varying levels of controls available to users. For example, the MindBody privacy policy stated that it collected location data from devices (through settings activated by the user) and IP address for service provision, delivery of content tailored to location, delivery of relevant marketing or advertising content, protection against misuse or abuse of the services or account, and to improve the site and its services. The user is given the option of disabling the location tracking through the browser, operating system or device settings. No instructions are provided for how a user would go about removing location tracking.[95] Snapchat collects location information and, if given permission by the user, will use technologies like GPS, cell towers and Wi-Fi access points to obtain a more detailed location point.[96] LinkedIn obtains location information from the device or IP addresses. Consumers can opt-in to more detailed location tracking.[97]

2018 research conducted on behalf of CPRC found that 71% of consumers did not want their location data shared with third parties.[98]

2018 research conducted on behalf of CPRC found that 71% of consumers did not want their location data shared with third parties.[98] At the same time, the pending rollout of world-leading 5G technology in Australia will enable location tracking with far greater accuracy than 4G networks, potentially down to the building an individual is located in.[99] Australia will be an early supplier of 5G services with network deployments already initiated by mobile operators.[100] Consequently, soon-to-be-introduced technology will have the capability of increasing the granularity of location tracking while the majority of Australians have already indicated that they would prefer to not have their location disclosed. This situation highlights how important it is for policy makers to understand the full ramifications of technology developments within increasingly short timeframes.

95. MindBody Privacy Policy (31 December 2018) "3. How we collect information" (https://www.mindbodyonline.com/privacy-policy) (accessed 13 February 2019)
96. Snapchat Privacy Policy (1 October 2018) "Information We Get When You Use Our Services" (https://www.snap.com/en-US/privacy/privacy-policy/) (accessed 13 February 2019)
97. LinkedIn Privacy Policy (8 May 2018) "1.5 Your Device And Location" (https://www.linkedin.com/legal/privacy-policy?trk=uno-reg-guest-home-privacy-policy#collect) (accessed 13 February 2019)
98. Nguyen P. and Solomon L. (2018) Consumer Data and the Digital Economy, Melbourne: Consumer Policy Research Centre, p.60 (http://cprc.org.au/2018/07/15/report-consumer-data-digital-economy/)
99. Grothaus, M. (3 january 2019) "5G means you'll have to say goodbye to your location privacy" Fast Company (https://www.fastcompany.com/90314058/5g-means-youll-have-to-say-goodbye-to-your-location-privacy)
100. Dent, J. (22 February 2019) "When can you get 5G in Australia?" WhistleOut (https://www.whistleout.com.au/MobilePhones/Guides/when-can-you-get-5G-in-Australia)

Consumer control

Policies offered varying levels of consumer control over the collection and use of their data, often requiring click-throughs to other sites without a clear explanation on the process for removing consent and vague statements that:

- This will cease some, but not all, of the data collection or use practices, or
- In some cases, removing consent to collect or use data will affect the quality of the data or mean that a service will not be able to be provided.

Many of the policies allow the user to opt-out from targeted advertising and direct marketing, but there is no ability to opt-out of the use of collection of personal information that may support those functions or from the use of user de-identified data for analytics purposes. For example, the Visa Global Privacy Notice allows users to opt-out of having their transaction data used to create “certain anonymised and aggregated marketing products”. This does not suggest that users can opt-out of all data uses. The user is provided with a link in the privacy policy that redirects to a "Opt-out of Interest-based Advertising" website housed by the Network Advertising Initiative Opt-Out page.[101] This suggests that this opt-out option relates to targeted advertising only.

Some privacy policies were very unclear about the level of consumer control over data collection that was possible. For example, the Woolworths Group privacy policy contains instructions on accessing and correcting personal information and specifically allows customers to opt-out of direct marketing, but no ability to stop the use and sharing of customers' anonymised information.[102] We believe that these kinds of unfair terms and practices leave consumers with very little control or choice over what happens to their personal information once these services have been engaged.

Many of the policies allow the opt-out from targeted advertising and direct marketing, but there is no ability to opt-out of the use of collection of personal information that may support those functions or from the use of user de-identified data for analytics purposes.

101. Visa Global Privacy Notice (23 May 2018) “10. Your Choices” (https://www.visa.com.au/legal/global-privacy-notice.html) (accessed 24 May 2019)
102. Woolworths Group Privacy Policy (January 2018) "Why do we collect, hold, use and disclose personal information?" and “How can you enquire about, access and correct your personal information?” (https://www.woolworthsgroup.com.au/page/privacy-policy/) (accessed 24 May 2019)

Harms

The data collection landscape and privacy policy analysis chapters describe an environment where there is substantial information asymmetry and power imbalance between consumers and the firms delivering the services they use. CPRC and Greater Than X partnered to identify harms.

There are a range of harms that emanate from this situation, both from:

- The collection and storage of the data itself, and
- The sharing and use of that data.

Tracking consumer preferences has always been possible, through loyalty cards, email newsletters, transaction data and other methods. However, technology is now allowing the tracking of consumers with far greater precision, at a volume and velocity never before possible. This enables marketers to advertise with increased accuracy and effectiveness, but also potentially creates new or more severe harms.[103] At a basic level, the granular level of tracking of sensitive personal information enabled by technology developments can result in a significant breach of privacy. Back in 2012, the New York Times reported that US store Target used customer profiling data – collected from a unique ID number tied to a customer's credit card, name or email address – to predict that a person is pregnant. Transaction data, such as the purchase of unscented lotion and supplements like calcium and zinc, was used to infer pregnancy. Based on this information Target began sending baby item coupons to users who were likely to be pregnant. In one incident, a teenager's family members found out about her pregnancy because she was sent these coupons.[104] While there may not have been negative economic ramifications from such a discovery, at a fundamental level this was a breach of the teenager's privacy, which no doubt caused significant stress and psychological harm.

Discussions of data collection practices tend to focus on the annoyance of, or preference for, targeted advertising. The real harms are more serious and include exclusionary and discriminatory practices as well the risk of manipulation and loss of autonomy as automated decision-making based on online profiles becomes increasingly commonplace.

Manipulation

Technological developments have enabled far greater monitoring of consumer behaviour and mood, including:

- Development of software that analyses eye movements and facial muscles to identify human emotions.[105]
- Inference of mood and other indicators via service usage. For example, Spotify shares information including their user's mood, listening behaviour and location.[106]
- Mobile phone sensors can infer information including mood, personality, stress levels, relationship status, employment status, mental health issues, sleep and physical movement.[107]

103. Manwaring, K. (2017) "Will emerging technologies outpace consumer protection law? The case of digital consumer manipulation" Competition & Consumer Law Journal, 26, p.2
104. Hill, K. (16 February 2012) "How Target Figured Out a Teen Girl was Pregnant Before Her Father Did" Forbes (https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#43a8159c6668)
105. Harari, Y. N. (2018) Twenty-one lessons for the Twenty-First Century UK: Penguin Random House, p.50
106. Thedataalliance.com cited in Christl, W. (June 2017) Corporate Surveillance in Everyday Life, p. 17 (https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf)
107. Peppet, S.R. (2014) "Regulating the Internet of Things" cited in Manwaring, K. (2017) "Will emerging technologies outpace consumer protection law? The case of digital consumer manipulation" Competition & Consumer Law Journal, 26

A number of researchers have voiced concern that this information is being used to influence the behaviour of consumers. For example, research found that the information and power asymmetry present in many sharing economy services gave these services the capacity to not only monitor the customers and the suppliers using the app, but also influence their behaviour.[108]

These developments represent a real risk of a loss of autonomy for consumers where, unbeknownst to them, their online profile is used by companies to make decisions about their treatment or eligibility. The potential for consumers to be manipulated through their online profiles may also reduce competition depending on who has access to the data and have privacy implications.[109] For example, as described earlier, the US store Target monitored its customers to the extent that it could identify pregnant customers. Originally Target sent consumers baby-related product coupons when their online profile suggests those customers were pregnant. The store quickly realised that customers were disturbed to receive these coupons when they hadn't revealed to Target that they were pregnant. Target changed its behaviour, interspersing baby-related coupons with other coupons so that the advertisements looked random and the customer did not realise Target knew that they were pregnant. This increased customer take-up of coupons.[110]

Regulators have recognised that consumer manipulation arising out of online tracking is a real risk. The European Data Protection Supervisor stated that this type of manipulation is a "threat to society".[111] In addition, one of the grandfathers of behavioural economics, Cass Sunstein recently released his "Bill of Rights of Nudging", acknowledging the need for a greater ethical lens to be applied by those implementing behavioural nudges. The Bill recommends five core principles be adopted:

1. Nudges must be consistent with people's values and interests,
2. Nudges must be for legitimate ends,
3. Nudges must not violate anyone's individual rights,
4. Nudges must be transparent, and
5. Nudges ought not to take thing from people without their consent.

The last principle is particularly important when considering the use of defaults. Where data collection sharing arrangements are set by companies to "on" by default this does result in a loss of personal information and data without a consumer's express consent. This loss of agency is something that should be considered closely by businesses and policymakers when designing consumer consent interfaces.[112]

Tracking consumer preferences has always been possible, through loyalty cards, email newsletters, transaction data and other methods. However, technology is now allowing the tracking of consumers with far greater precision, at a volume and velocity never before possible.

108. Calo, R. and Rosenblat, A. (9 March 2017) "The Taking Economy: Uber, Information, and Power" Columbia Law Review, Vol. 117, University of Washington School of Law Research paper No. 2017-18 (https://dx.doi.org/10.2139/ssrn.2929643)
109. Manwaring, K. (2017) "Will emerging technologies outpace consumer protection law? The case of digital consumer manipulation" Competition & Consumer Law Journal, 26, p.9
110. Hill, K. (16 February 2012) "How Target Figured Out a Teen Girl was Pregnant Before Her Father Did" Forbes (https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#43a8159c6668)
111. Manwaring, K. (2017) "Will emerging technologies outpace consumer protection law? The case of digital consumer manipulation" Competition & Consumer Law Journal, 26, p.10
112. Easton, S. (19 July 2018) "Cass Sunstein's Bill of Rights for Nudging" The Mandarin (https://www.themandarin.com.au/96009-cass-sunsteins-bill-of-rights-for-nudging/)

Discrimination and exclusion

Discriminatory and exclusionary harms from online profiles are already happening. Consumer profiles are used to support automated decision-making in finance, insurance, employment and other industries. For example, some organisations are using data including location, purchase histories, web search, and social networks information to build creditworthiness profiles of individuals.[113] "E-scores" – which are based on a user's online behaviour and usage – are used by services like Credit One to determine the advertisements shown to the user.[114]

Other measurements include "customer's lifetime value", which is used to identify and retain profitable customers.[115] US insurers have reportedly begun using algorithms to look at non-traditional consumer information in determining insurance access and cost. This information includes social media activity, photographs, location tracking and retail transactions.[116] The lack of transparency and accountability of these systems makes it difficult for consumers to appeal decisions or correct assumptions based on wrong information.[117]

Opting-out of having an online presence doesn't prevent these outcomes and may actually reduce access to certain products in the future as automated decision-making becomes ubiquitous across the economy. For example, insurance coverage may in future become dependent on access to personal healthcare data.[118] The risks related to health data and potential discriminatory harms is particularly important. 2019 research analysing the top 24 medicines-related apps for Android found that these apps routinely share information in ways that are not transparent to the user. The research also identified some commercial entities that would have the ability to aggregate and potentially re-identify that data.[119]

In 2018, the popular gay dating network app Grindr was shown to be revealing users' HIV status to third parties, violating users' privacy but also making them vulnerable to discrimination. The practice has since ceased.[120] The mobile app, Ovia, is a fertility and pregnancy tracker where users frequently input detailed health information including medications and mood. Ovia then sells this information, in a de-identified and aggregated form, to the employers of the users. Data that could be accessed by employers include how many workers had high-risk or premature births, the medical questions they had researched, and when they were planning on returning to work. The risks from this type of app are numerous: data leakage from breaches, price discrimination in health coverage, and workplace discrimination if employees are re-identified.[121]

Opaque sharing of health-related data can have a real influence on consumers' access to, and the cost of, services such as insurance. Health information is also very sensitive, and the leakage of information such as HIV status, could have profound social and economic implications for individuals.

113. Christl, W. (June 2017) Corporate Surveillance in Everyday Life, p. 79 (https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf)
114. O'Neil, C. (2016) Weapons of Math Destruction USA: Crown Books, p. 143
115. Christl, W. (June 2017) Corporate Surveillance in Everyday Life, p. 13 (https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf)
116. Heller, N. (26 February 2019) "Why the Life-Insurance Industry Wants to Creep on Your Instagram" New Yorker (https://www.newyorker.com/culture/cultural-comment/why-the-life-insurance-industry-wants-to-creep-on-your-instagram)
117. O'Neil, C. (2016) Weapons of Math Destruction USA: Crown Books
118. Harari, Y. N. (2018) Twenty-one lessons for the Twenty-First Century UK: Penguin Random House, p.79
119. Fergus, R. (21 March 2019) "Data sharing by popular health apps is 'routine', research finds" The University of Sydney (https://sydney.edu.au/news-opinion/news/2019/03/21/data-sharing-by-popular-health-apps-is--routine---research-finds.html)
120. Belluz, J. (3 April 2018) "Grindr is revealing its users' HIV status to third-party companies" Vox (https://www.vox.com/2018/4/2/17189078/grindr-hiv-status-data-sharing-privacy)
121. Harwell, D. (10 April 2019) "Is Your Pregnancy App Sharing Your Intimate Data With Your Boss?" The Washington Post (https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/?utm_term=.e3825c86adb3)

Even more concerningly, consumers may well start to avoid accessing important healthcare services and support if they feel that companies or governments cannot be trusted with that information, or that they may be disadvantaged by that information in future. For example, insurer MLC was found to have excluded a consumer from mental health coverage in life insurance due to her accessing mental health services for the sexual abuse she suffered as a child in the mid-1980s.[122] Location tracking (in a 5G environment) in particular may provide insights into the frequency and types of healthcare services that an individual might be accessing, regardless of whether formal medical records are being accessed.

The lack of transparency around data collection practices means that consumers have no way to check whether the information shared about them is correct or to appeal decisions made on that information. Consumers don't see the processes that influence their profile based on their online and offline behaviour, or the impact of these online decisions in the short and long term.[123] This frustrates the ability of consumers to appeal discriminatory or exclusionary decisions made about them. In addition, the possibility that there are errors in the online profile intensifies the risks of wrong or exclusionary decisions. Errors are relatively commonplace. For example, a 2014 article noted that personal characteristics – such as gender and age – inferred from Google's search histories were often wrong.[124]

Consumers don't see the processes that influence their profile based on their online and offline behaviour, or the impact of these online decisions in the short and long term.[123]

Personal security

The technology journalist Jason Koebler asserts people are no longer the weakest link in their own security, rather it is the infrastructure that collects and controls personal data without allowing users the chance to control that process.[125] New data breaches are announced every month, demonstrating that data storage can be a harm on its own. Breaches at Equifax, Facebook and the US Office of Personnel Management have all resulted in the leaking of personal data.[126] In 2018, it was discovered that Exactis, a data broker, was storing a database holding around 340 million individual records on a publicly accessible server. Data included phone numbers, emails, personal interests, and family make-up.[127] A Nest camera was hacked in California and "broadcast fake audio warnings about a missile attack".[128]

Location data is one example of how data collection poses real personal security risks. ACCC research found extensive ability to track locations within several digital platform's privacy policies. For example, Google "allows the collection of user location data via GPS, IP addresses, sensor data from the user's mobile device, and information from Wi-Fi access points, cell towers, and Bluetooth-enabled devices". Facebook also collects location information.[129]

122. Bainbridge, A and Clark, E. (24 January 2019) "Insurers gaining 'open-ended access' to medical records slammed as 'unfair privacy breach'" ABC News (https://www.abc.net.au/news/2019-01-24/medical-records-handed-to-insurance-companies-over-mental-health/10720024)
123. Christl, W. (June 2017) Corporate Surveillance in Everyday Life, p. 67 (https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf)
124. Duhaime-Ross, A. (19 September 2014) "Here's how well Google's search engine knows you" The Verge (https://www.theverge.com/2014/9/19/6409773/heres-how-well-googles-search-engine-knows-you)
125. Koebler J (13 November 2018) "The weakest link in cybersecurity isn't human, it's the infrastructure" Motherboard VICE (https://www.vice.com/en_us/article/d3bvgy/the-weakest-link-in-cybersecurity-isnt-human-its-the-infrastructure)
126. Kemp, K. (27 September 2018) "Getting Data Right" Center for Financial Inclusion (https://www.centerforfinancialinclusion.org/getting-data-right)
127. Greenberg, A (27 June 2018) "Marketing firm Exactis leaked a personal info database with 340 million records" Wired (https://www.wired.com/story/exactis-database-leak-340-million-records/)
128. Fowler, G. A. (31 January 2019) "The Doorbells Have Eyes: The Privacy Battle Brewing Over Home Security Cameras" The Washington Post (https://www.washingtonpost.com/technology/2019/01/31/doorbells-have-eyes-privacy-battle-brewing-over-home-security-cameras/?utm_term=.de9ff39e42e4)
129. ACCC (December 2018) Digital Platforms Inquiry Preliminary Report, p. 189 (https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry/preliminary-report)

Disclosure of location related information, such as travelling routes to work or dropping the kids off at school, can jeopardise an individual's physical safety. This can be gleaned from EXIF data (metadata) on people's images they post on social media and also through more sophisticated means if the attacker/adversary is intent on causing harm and has the means to get access to additional information. There is also potentially sensitive information that can be inferred from location data. A New York Times article outlining the capabilities of device location tracking showed a user arriving at a Planned Parenthood clinic and staying for two hours. While this type of information is attached to a unique ID, rather than a phone number or name, there are other ways to identify the person. For example, this includes using public records to identify the person living at a residence where an anonymous device spends every night.[130]

Consumer trust

Previous CPRC consumer research has indicated that consumers are uncomfortable with the amount of information collected about them and their lives and would prefer to have greater control over that data collection.[131] The opaqueness of data collection practices has a negative influence on consumer trust.

One example is the use of personal photos to improve facial recognition technologies. IBM has promoted its holding of a set of almost one million photos sourced from Flickr as a tool to reduce bias in facial recognition technologies. Individuals notified by NBC News that their photographs had been included in this set expressed surprise and concern. One person, who had more than 700 of his photos included in the collection, commented, "None of the people I photographed had any idea their images were being used in this way" and "It seems a little sketchy that IBM can use these pictures without saying anything to anybody".[132]

It is also difficult to build consumer trust in organisations that are handling consumer data but are not consumer facing. The 2014 US Federal Trade Commission's Data Brokers report found that the nine data brokers studied sourced their information from other data brokers rather than directly from consumers. The breaking of the service chain to remove consumers is potentially detrimental to consumers. For example, as data brokers are not consumer facing, it is difficult for consumers to know where and how to remove their associated data from the brokers' holdings. The Data Brokers Report found that consumers who were able to find the data brokers and request to opt-out are likely to find the opt outs provided confusing and be unsure of its limitations.[133]

Consumer awareness that an individual's online behaviour may influence future opportunities may affect behaviour. This "social cooling" effect may range from minimising the number of visits to a travel site in case it increases flight prices to restricting speech or nonconforming behaviours that may influence their online profile and affect their access to services.[134]

130. Valentino-DeVries, J., Singer, N., Keller, M.H. and Krolik, A. (10 December 2018) "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," The New York Times. (https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html)
131. Nguyen, P. and Solomon, L. (2018) "Consumer data and the digital economy" Consumer Policy Research Centre. p. 32 (http://cprc.org.au/wp-content/uploads/Full_Data_Report_A4_FIN.pdf)
132. Solon, O. (12 March 2019) "Facial recognition's 'dirty little secret': Millions of online photos scraped without consent" NBC News (https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921)
133. Federal Trade Commission (May 2014) "Data Brokers. A Call for Transparency and Accountability" Federal Trade Commission, p.49 (https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf)
134. Christl, W. (October 2017) "How companies use personal data against people" Cracked Labs, p.23-25 (https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf)

Children

The data collection, sharing and use process has special harms for children, as recognised by the GDPR which prohibits the processing of data about children under the age of 16 without parental consent in relation to the offer of information society services directly to a child. Children are unlikely to understand the risks and consequences to their privacy of their behaviour online. In addition, an online profile built on a child may result in inferences included in that profile that will affect their future as an adult. Despite prohibitions against collecting children's data, it appears to still occur frequently. An analysis of mobile phone apps found that the majority of the 5,855 most popular children's apps were potentially in violation of the Children's Online Privacy Protection Act due to their use of third-party Software Development Kits (SDKs). While many SDKs do provide options to disable tracking of children, the majority of the apps do not make use of these settings, or use them incorrectly.[135]

In other cases, the New Mexico Attorney General recently announced a lawsuit against various technology companies for illegally tracking children online.[136] This widespread undercover tracking of children and their behaviour poses potentially serious harms for these children's autonomy and future opportunities as they mature into adults. Children's personal information is often shared online as a result of decisions by adult members of their family, rather than through independent choice. For example, it is common for proud parents to post photos of their young children on social media platforms as a way to update family and friends on their child. As a result, children have generated online profiles well before they are legally able to drive, vote, marry or be considered an adult in a court of law. If we are to respect the right to privacy during these important developmental years, it is essential that children under the age of eighteen have a right to have that information deleted, not processed or used by companies.

An analysis of mobile phone apps found that the majority of the 5,855 most popular children's apps were potentially in violation of the Children's Online Privacy Protection Act due to their use of third-party Software Development Kits (SDKs).[135]

135. Reyes, I, Wijesekera, P, Reardon, J, Bar On, A E, Razaghpanah, A, Vallina-Rodriguez, N and Egelman, S. (2018) "'Won't Somebody Think of the Children?' Examining COPPA Compliance at Scale" Proceedings on Privacy Enhancing Technologies, pp.63-83 (https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf)
136. New Mexico Attorney General (12 September 2018) "AG Balderas Announces Lawsuit Against Tech Giants Who Illegally Monitor Child Location, Personal Data" Presse Release (https://www.nmag.gov/uploads/PressRelease/48737699ae174b30ac51a7eb286e661f/AG_Balderas_Announces_Lawsuit_Against_Tech_Giants_Who_Illegally_Monitor_Child_Location__Personal_Data_1.pdf)

Policy responses

While these harms – such as power and information imbalance – are not new, the velocity and scope of digital transformation is creating distinctive policy challenges.[137]

The growing harms from the information and power imbalance between data collectors or holders and consumers requires a coordinated and significant policy response.

Consumers appear uncertain about what information is collected, shared and used about them online and offline. The opaqueness of the data brokerage market exacerbates this information imbalance. This environment is debilitating for consumer confidence and trust, raises the risk of instilling further social and economic inequality, and prevents consumers from making informed choices about their personal information. While these harms – such as power and information imbalance – are not new, the velocity and scope of digital transformation is creating distinctive policy challenges.[137]

Governments and businesses globally are recognising the place for government intervention in this sector. Leaders of China, Japan, South Africa and Germany have expressed interest in a global approach to the technology sector, including data governance.[138] Satya Nadella, the CEO of Microsoft, this year stated that government regulation of facial recognition will be required to prevent harmful consequences and that a good place to start would be to acknowledge privacy as a human right.[139] At the recent World Economic Forum in Davos he also shared his view that the default had to be that consumers owned their own data, and IBM CEO Ginni Rometty agreed, calling for a new era of data responsibility.[140]

Policy responses will intersect across competition, consumer protection, privacy legislation and human rights concerns. Jurisdictions worldwide are testing interventions across these overlapping areas. For example, the EU has implemented general data protections via the GDPR. At the same time national competition authorities within Europe are issuing orders aimed at preventing data monopolies. Bundeskartellamt, the German competition authority, issued an order in February 2019 to stop Facebook combining its own users' data with Instagram, WhatsApp and third-party data.[141]

This section highlights some policy responses to data collection and use across the areas of transparency, comprehension, control, accountability and minimum protection standards. CPRC will continue to explore the optimal policy levers that could be used to respond to the data collection ecosystem in future papers.

137. OECD Digital Economy Papers (January 2019) "Vectors of Digital Transformation" p.29 (https://www.oecd-ilibrary.org/science-and-technology/vectors-of-digital-transformation_5ade2bba-en)
138. Bradsher K. and Bennhold K. (23 January 2019) "World Leaders at Davos Call for Global Rules on Tech" The New York Times. (https://www.nytimes.com/2019/01/23/technology/world-economic-forum-data-controls.html)
139. Browne R. (24 January 2019) "Microsoft CEO says facial recognition technology needs to be regulated" CNBC.COM (https://www.cnbc.com/2019/01/24/davos-microsofts-nadella-says-facial-recognition-needs-regulation.html)
140. Parker C. (24 January 2019) "Privacy is a human right, we need a GDPR for the world: Microsoft CEO" World Economic Forum (https://www.weforum.org/agenda/2019/01/privacy-is-a-human-right-we-need-a-gdpr-for-the-world-microsoft-ceo/)
141. Van Dorpe, S. (7 February 2019) "German competition authority orders Facebook to change data collection procedures" Politico (https://www.politico.eu/article/german-competition-authority-orders-facebook-to-change-data-collection-procedures/

Transparency

The opacity of data collection practices restricts consumers' ability to make informed decisions and governments' ability to understand the markets they are regulating and formulate appropriate policy responses. Transparency will be the building block for any policy solution to address harms from data collection sharing and use and to support the beneficial outcomes of these practices.

Governments around the world are attempting to inject some transparency in different ways. Vermont in the US has introduced laws to regulate data brokers that will require them to register with the Vermont Attorney General, require data brokers to report annually regarding data privacy practices and data breaches to develop written information security programs.[142] In the UK, the Chancellor has recommended a study of the UK digital advertising market partly due to its lack of transparency.[143] The ACCC in Australia has released the Digital Platforms Inquiry Preliminary Recommendations Report that provides a comprehensive spotlight on the data collection, sharing and use practices of digital platforms.[144]

Transparency will be the building block for any policy solution to address harms from data collection sharing and use and to support the beneficial outcomes of these practices.

Our research finds three core aspects of transparency as a fundamental building block to an effective data economy:

- **Data collection, sharing and use practices must be clear and understandable for consumers to make informed choices**

The significant level of opacity inherent in current disclosure of data collection, sharing and use practices in Australia has been well documented within this report and in many others. Most importantly, the ACCC Digital Platforms Inquiry Preliminary Report concluded that significant market and regulatory failure in the Australian policy environment has led to consumers being unable to make informed choices about their data and personal information.

Greater transparency will be fundamental if consumers are to continue to be relied upon to make informed choices about the products and services they are purchasing and engaging with.

Consistent with prior CPRC research[145], we find that a lack of service quality information restricts consumers' capacity to differentiate between high quality and low quality service providers. Thus, wherever quality disclosure (in this case privacy) is hidden, we observe a weakening in competition for high quality products and services and an overreliance by consumers on brand as an imperfect proxy for quality. This is certainly anecdotally the case. While the Australian market for pro-privacy or pro-data ethics products and services is muted, in jurisdictions such as the EU this sector is undergoing major growth. Reforming Australia's Privacy Act to ensure that greater transparency is delivered for all in the ecosystem must be a fundamental first step.

- **Greater transparency of the data supply chain is required for policy makers and regulators to design effective and fit-for-purpose interventions**

One of the major challenges globally with the regulation of data collection, sharing and use is that the ecosystem itself is not well understood. Traditional economic models have not been effective when considering the movement of data and personal information from homes to around the economy.

142. Serrrato, J. K., Cwalina, C., Rudawski, A., Coughlin, T. and Fardelmann, K. (9 July 2018) "US states pass data protection laws on the heels of the GDPR" Norton Rose Fulbright (https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/)
143. Sweney, M. (13 March 2019) "Hammond calls for regulator to investigate UK's digital ads market" The Guardian (https://www.theguardian.com/media/2019/mar/13/hammond-calls-for-regulator-investigation-uk-digital-ad-market-facebook-google)
144. ACCC (December 2018) Digital Platforms Inquiry Preliminary Report (https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry/preliminary-report)
145. Martin Hobbs B (2018) "But are they any good" The value of service quality information in complex markets. Consumer Policy Research Centre. (https://cprc.org.au/wp-content/uploads/CPRC-2018-But-are-they-any-good.pdf)

One of the key considerations is the extent of market power now held by firms with vast amounts of personal information. For example, many jurisdictions have voiced concerns about large digital players effectively creating data monopolies out of their users' data that through network effects and other factors creates extremely high barriers to entry in those markets.[146] Effective regulation of the ownership of data will be key to preventing a concentration of wealth and power in the few.[147] Governments require new understandings of market boundaries, the products and services they comprise and their associated supply chains in order to assess the state of competition.

The data economy is built on a constant supply of consumer data.

- **Increased knowledge of the flow of data will be central to better understanding the value of data as a growing input to production**

Most importantly, transparency in market practices will be the first step in assessing the value of data for both consumers and governments. There is a growing explicit recognition of the value of data, with Google and Facebook reportedly paying people to download an app that tracks all their phone activity and usage habits.[148] This shows that data is of value to digital platforms, but currently it is only those services that can set the price.

At present, consumers are unsure of what information they are giving away, and what that data will be used for. It is also unclear whether the value of the data will change over time, for example if it is incorporated into a more detailed online profile or aggregated with other consumer datasets to support an algorithm. Consumers cannot be expected to provide informed consents when they don't understand what they are consenting to. For both parties, understanding the value of the data is dependent upon understanding the collection, sharing and use of that data between all participants in the supply chain. The OECD has explored a range of market and consumer-based methodologies for estimating the value of data, including the cost of a data breach, market prices for data, the willingness of an individual to pay to protect their data.[149] All of these methodologies require basic market transparency in order to be effective and accurate.

Existing and forthcoming research can be used to support the next stage of discussion: the value of the data across the supply chain, and who should be sharing in that value. Better understanding of the value created by the collection and processing of data along the supply chain will enable more realistic assessments of the value of the services offered compared to value of the data collected from the users.

Lastly, transparency will be key to building consumer trust, which in turn will ultimately determine whether consumers continue to allow their data to be collected or, take steps to avoid or falsify that information. Or worse, avoid engaging services that they might desperately need. The data economy is built on a constant supply of consumer data. For us all to benefit from the good that this data can provide, it's going to be essential to work in partnership with consumers, respecting their fundamental rights for this supply to continue.

146. Zuboff, S. (2019) The Age of Surveillance Capitalism New York: Hatchette Book Group
147. Harari, Y. N. (2018) "Twenty-one lessons for the Twenty-First Century" UK: Penguin Random House, p.77
148. Editorial Board (2 February 2019) "How Silicon Valley Puts the 'Con' in Consent", The New York Times (https:www.nytinmes.com/2019/02/02/opinion/internet0facebook-google-consent.html)
149. OECD (2013) "Exploring the economics of personal data: A Survey of Methodologies for Measuring Monetary Value" OECD Digital Economy Papers. No. 220. Paris: OECD Publishing, p.19 (https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en)

Consumer comprehension and control

Transparency of the collection, sharing and use of personal data alone does not necessarily mean that consumers will understand, or be able to alter, the contract they are entering into when using an online service. This information also needs to be comprehensible to consumers. Our analysis of privacy policies (p25) demonstrates that these documents are often vague and hard to understand for the average consumer. Privacy policies are also offered on a "take-it or leave-it" basis, with little option to alter the data collection arrangements.

Internationally, there are different approaches to giving consumers more control over their data and implementing meaningful consent requirements. The EU and California have introduced data protections legislation that outline notification and disclosure requirements. The GDPR affirms consumers rights around their data and places obligations – including transparency – on those entities processing that data.[150] The California Consumer Privacy Act gives consumers the right to opt-out of their information being sold to third parties and the right to be forgotten.[151]

In Australia, the ACCC's Digital Platform Inquiry recommends strengthening consent requirements in the Privacy Act. These recommendations include requirements for consent to be provided expressly, specific to purpose, easy to understand, easily accessible, able to be withdrawn, and freely given. The Inquiry further recommends that service settings that enable data collection should be pre-selected to off.[152] CPRC strongly supports these recommendations and considers that the consent and default settings requirements should apply economy-wide, rather than only to digital platforms. 2018 CPRC research found that only 27% of Australians found the process of passively collecting data from websites to support targeted advertising acceptable.[153] Consequently, setting data collection to be 'off' as the default would bring Australian regulation in line with community expectations.

Education will also be a core policy lever to give consumer more understanding and control over their data. However, it is difficult to adequately educate consumers when the market structure and commercial practices are opaque, governments do not understand the environment and consumers have limited control.

In Australia, the introduction of a Consumer Data Right – if coupled with adequate reform of the Privacy Act to increase protections – could provide consumers greater control over the portability of their consumer data. Other approaches to increase consumer control have included the establishment of a central database of information. For example, a central information bank has been set up in Japan. The bank stores consumer data held by government and companies. Consumers with information held in the bank can select what uses of their data they will consent to.[154]

Transparency of the collection, sharing and use of personal data does not mean that consumers will understand, or be able to alter, the contract they are entering into when using online service.

150. Zuiderveen Borgesius, F. (2018) "Discrimination, artificial intelligence, and algorithmic decision-making" Council of Europe, p.21 (https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73)
151. Serrrato, J. K., Cwalina, C., Rudawski, A., Coughlin, T. and Fardelmann, K. (9 July 2018) "US states pass data protection laws on the heels of the GDPR" Norton Rose Fulbright https://www.dataprotectionreport.com/2018/06/california-passes-major-privacy-legislation-expanding-consumer-privacy-rights/
152. ACCC (December 2018) Digital Platforms Inquiry Preliminary Report, pp.13-14 (https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry/preliminary-report)
153. Nguyen, P and Solomon, L (2018) Consumer data and the digital economy, p. 34 (https://cprc.org.au/publication/consumer-data-and-the-digital-economy-report/)
154. Nikkei Asian Review (24 February 2017) "Japan takes step toward enormous bank of personal data" (https://asia.nikkei.com/Economy/Japan-takes-step-toward-enormous-bank-of-personal-data)

Accountability

The collection, sharing and use of data supports automated decision-making that is increasingly used by a range of sectors and provides a limited ability for consumers to understand the reasons for the decision, the data used to do so, or appeal the outcome. Policy responses to make these practices accountable to consumers, and to ensure that the use of data is designed in line with social benefits rather than exacerbating existing social inequities are also important. For example, the notion of ethical use of or "fair" outcomes from the algorithms support Artificial Intelligence systems can be subjective.[155] AIgorithms should consequently be able to be interrogated to test the fairness of their assumptions and outcomes.

Policy responses to make these practices accountable to consumers, and to ensure that the use of data is designed in line with social benefits rather than exacerbating existing social inequities are also important.

Various jurisdictions have been exploring how the use and outcomes of consumers' data could be explained, including stronger enforcement processes and providing a guide on inclusive design for sustainable innovation. In the UK, the Centre for Data Ethics and Innovation in the UK will develop best practice guidance for ethical and innovative uses of data.[156] There have been a range of publications establishing theoretical frameworks for the ethical collection, sharing and use of user data. For example, the recent QUT publication, Good Data, discusses good data practices designed to support "a fair and just digital economy and society."[157] As part of this work, a set of Good Data Principles have been identified that address issues of consumer control over their own data, empowering citizens, and justice. Some of these principles addressed good data practices:

- Data should be usable and fit for purpose,
- Data should respect human rights and the natural world, and
- Good data should be published, revisable and form useful social capital where appropriate to do so.[158]

Cass Sunstein's "Bill of Rights of Nudging"[159] include the concept that: *Nudges should not take something away from someone without their consent.* In the context of data collection sharing and use practices, we interpret consent to mean that which is voluntary, freely given, active, able to be withdrawn, and specific to purpose. Thus, where these fundamental components of consent are not present and vast amounts of data about an individual is collected and used by companies, such a practice would be deemed unethical by this Bill of Rights.

Another aspect of accountability will be the "right to explanation". At present, explanations for automated decision-making may not be available to the consumers affected. For example, Basix, a financial company offering personal and small business loans, denotes applicants who fill in their names in all caps as higher risk. A spokesman for the company was unable to explain why this data point indicated a higher risk customer.[160] As automated decision-making becomes more common, requiring a right to explanation will be a partial check against discriminatory decision-making as well as outcomes based on information containing errors.

155. Spielkamp, M. (12 June 2017) "Inspecting algorithms for bias" MIT Technology Review (https://www.technologyreview.com/s/607955/inspecting-algorithms-for-bias/)
156. Department for Digital, Culture, Media and Sport (20 November 2018) "Consultation outcome. Centre for Data Ethics and Innovation Consultation." (https://www.gov.uk/government/consultations/consultation-on-the-centre-for-data-ethics-and-innovation/centre-for-data-ethics-and-innovation-consultation#the-centres-role-and-objectives)
157. Mann, M., Devitt, K. and Daly, A. (2019) "What Is (In) Good Data" In Daly, A., Devitt, K., and Mann, M. (Eds.) Good Data Amsterdam: Institute of Network Cultures (https://eprints.qut.edu.au/123773/)
158. Dubbeldam, B. (11 January 2019) "Principles of 'Good Data'" Network Cultures (http://networkcultures.org/blog/2019/01/11/principles-of-good-data/)
159. Easton, S. (19 July 2018) "Cass Sunstein's Bill of Rights for Nudging" The Mandarin (https://www.themandarin.com.au/96009-cass-sunsteins-bill-of-rights-for-nudging/)
160. Koren, J. R. (19 December 2015) "Some Lenders are Judging You on Much More than Your Finances" Los Angeles Times (https://www.latimes.com/business/la-fi-new-credit-score-20151220-story.html?outputType=amp&__twitter_impression=true)

Minimum protection standards

Increasingly, there also seems to be some growing consensus that there are also some types of data collection, sharing and use practices that should simply not be allowed. Where unarguably bad outcomes from data collection, sharing and use can be identified, there may be scope to have these practices banned outright. For example, data protection standards like the GDPR do not allow the processing of data about minors.

Where unarguably bad outcomes from data collection, sharing and use can be identified, there may be scope to have these practices banned outright.

Minimum safety standards for privacy and data storage is another key tool in protecting consumers, to ensure that products and services deployed prevent the significant extraction of personal information and data, either directly or via a data breach through malicious attacks. For example, testing of smart products have revealed that their connections are vulnerable to hacking. A 2016 review of a fertility app, Glow revealed anyone with basic software skills would be able to harvest information from the app. The insecure data included email addresses, password, and health concerns.[161]

Hackers stole data from the CloudPets range of toys that enabled children to send and receive messages from their parents or loved ones. A security researcher found that CloudPets didn't use encryption or require authentication when sending and receiving the messages. He exploited the vulnerability by hacking a CloudPet to say "Exterminate, annihilate!" and turning the toy into a recording device.[162] These examples show the need for the implementation and enforcement of minimum security standards to protect individuals and particularly children.

161. Beilinson, J. (28 July 2016) "Glow Pregnancy App Exposed omen to Privacy Threats, Consumer Reports Finds" CR Consumer Reports (https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats/)
162. Vlahos, J. (26 March 2019) "Smart Talking: Are Our Devices Threatening Our Privacy" The Guardian (https://www.theguardian.com/technology/2019/mar/26/smart-talking-are-our-devices-threatening-our-privacy)

Powers to address unfair and exploitative practices

One aspect of these protections would be prohibiting unfair practices that exploit consumers. Policy makers have recognised that even the best educated consumer will still require protections against unfair business practices. In the US, Senator Brian Schatz introduced the Data Care Act in late 2018. The Bill includes a requirement for data holders to not use information held about consumers in a harmful way.[163] Additional suggestions for a Data Bill of Rights have included the right to not be the subject of unreasonable surveillance, the right to not have their behaviour manipulated, and the right to not be unfairly discriminated against.[164]

The EU Commission, European Parliament and the Council of the European Union have introduced rules that are aimed at preventing unfair trading practices by online platforms. These rules include a ban on account suspensions without clear reasons or opportunity to appeal, and a requirement for terms and conditions to be intelligible with at least 15 days notice given for changes. The ranking of products and services on an online platform must also be transparent for sellers on that platform.[165]

The ACCC's Digital Platforms Inquiry has included consideration of a provision to protect consumers against unfair trading practices as an area for further development. This could take the form of a general prohibition against the use of unfair trading practices in the Australian Consumer Law, which would enhance consumers' bargaining power in their contracts with service providers as well as encourage digital platforms to act in line with community expectations. General prohibitions on unfair trading practices are a complementary policy tool to ensuring consumers can provide informed consent. The combination of two policy responses are a recognition that consumers should not shoulder the entire responsibility of protecting themselves, but that there are situations where minimum protections should be in place.

General prohibitions on unfair trading practices are a complementary policy tool to ensuring consumers can make informed consent.

163. Lecher, C. (12 December 2018). "Democratic senators have introduced a big new data privacy plan" The Verge (https://www.theverge.com/2018/12/12/18138131/democratic-data-care-act-senate-law)
164. Tische, M. (14 December 2018) "It's Time for a Bill of Data Rights" MIT Technology Review (https://www.technologyreview.com/s/612588/its-time-for-a-bill-of-data-rights/)
165. European Commission (14 February 2019) "Digital Single Market: EU negotiators agree to set up new European rules to improve fairness of online platforms' trading practices" European Commission (http://europa.eu/rapid/press-release_IP-19-1168_en.htm)

Better business practices

Effective policy responses need to be coupled with a step-change in business practices to ensure ethical and transparent data collection, sharing and use. CPRC have engaged Greater Than X, a strategic advisory firm that specialises in data trust, data ethics and data privacy, to outline some core elements of ethical business design.

By committing to - and consistently delivering on - ethical, verifiably trustworthy behaviours, organisations can:

- Provide greater transparency and accountability,
- Improve comprehension of legal agreements and related data processing activities,
- Offer more effective control and choice to their customers,
- Decrease the risk and maximise the value of data sharing events, and
- Earn greater trust.

Greater Than X outlines some key business behaviours that support a transparent, customer first approach.

Lead with the information strategy

The most trusted organisations will become the most valued. The most trusted organisations will gain the greatest access to their customers.

This perspective must be prioritised at the very top of the organisation. It starts with boards evolving their skills, experiences and composition. Boards must become adept at setting competitive and ambitious information strategy, as well as effectively identifying and managing information risks.

The information strategy should be supported by specific tactics and measurements that give the entire organisation clear visibility of the tangible progress being made.

Although this requires significant change, the time for leadership is now.

Develop new metrics to determine success (and incentivise positive cultural change)

Metrics measuring organisational success are often misaligned to customers' actual concerns, as shown in the recent Royal Commission into Financial Services. The Commissioner Kenneth Hayne commented that, "rewarding misconduct is wrong. Yet incentive, bonus and commission schemes throughout the financial services industry have measured sales and profit, but not compliance with the law and proper standards".[166]

For organisations to value and effectively design for trust, they need to incentivise the behaviours that make ethical, trustworthy practices "normal". There are three specific customer metrics, in the context of information sharing, organisations can begin designing for today:

1. **Comprehension:** The ability for customers to accurately recall the key parameters of the agreement they've entered into,
2. **Time to Comprehension:** The time it takes from first interaction through to an active, informed decision being made by a customer, and
3. **Propensity to Share:** The willingness a customer has to enter into the agreement and share specific information based on their understanding of the value exchange, their rights and the measures that exist to protect them.

Designing for these outcomes empowers customers. Doing this effectively increases trust and willingness to share.

Enhance social preferability with an operationalised data ethics framework

Implementing a data ethics framework enables an organisation to decide which data processing activities are socially preferable, document those processes to ensure consistency, and then verify the outcomes. A data ethics framework defines what an organisation will and won't do. The consistent operation and verification of those processes:

- Holds the organisation accountable to those ethics framework-based decisions,
- Maintains alignment to customer outcomes, and
- Increases the likelihood the organisation's conduct is positive.

Ultimately, a data ethics framework supports a greater level of accountability.

Privacy is the default setting

Privacy and Security by Design is a well-established approach to proactive, person centric approaches to data privacy and security. These approaches have been endorsed by the International Association of Data Protection Authorities and Privacy Commissioners, the U.S. Federal Trade Commission, the European Union and privacy professionals globally.

The seven foundational principles of Privacy and Security by Design[167] affirm a culture of privacy and helps establish policies, requirements and practices that benefit customers and the business.

166. Hayne, K. (4 March 2019) "Kenneth Hayne's final royal commission report held back 'heavy hits' from the banks" ABC News (https://www.abc.net.au/news/2019-02-26/hayne-banking-royal-commission-squib/10832620)
167. Privacy by Design Centre of Excellence (Undated) "The Seven Foundational Principles" Ryerson University (https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/)

The implementation of these principles by organisations will:

- Enhance the likelihood consumers have more choice and control,
- Allow organisations to focus on balancing compliance obligations with data enabled innovation and business growth, and
- Help organisations to build greater trust with their customers.

Privacy Enhancing Technologies can also assist organisations in upholding their values, while managing compliance more simply and cost effectively. The suite of capabilities for Privacy Enhancing Technologies is broad, and includes:

- Data mapping and discovery tools,
- Consent management platforms, and
- Personal Information Management Services (PIMS) to name a few.

The International Association for Privacy Professionals publishes a yearly vendor report on this area for businesses to use.[168]

By collaborating with customers early and often, organisations increase the likelihood their data processing activities (intent and outcomes) are socially preferable.

Data trust, by design

Although Privacy and Security by Design ends with the word “design”, the principles rarely make their way to into service experiences. Data Trust by Design bridges the gap with principles, patterns and practices that directly contribute to all customer facing activities.

Operationalising these principles via distinct practices[169] supports the design of:

- Privacy notices and upfront terms and conditions that are easily comprehensible and supportive of informed decision making,
- Cookie notices and settings to enable consumer choice over the information that is passively collected and processed about them,
- Consent based data sharing interactions that specify purpose, support meaningful choice and deliver real value, and
- Broader data rights, like the right to be forgotten, that are being established in different jurisdictions.

Prioritise a culture of experimentation and collaboration

Organisations that value learning will experiment by design. This systematic approach to experimentation and collaboration – through a “Living Lab”– enables customers to actively opt in to an ongoing research program that helps shape the future of their interactions with a given organisation.

By collaborating with customers early and often, organisations increase the likelihood their data processing activities (intent and outcomes) are socially preferable.

168. International Association of Privacy Professionals (2019) “2018 Privacy Tech Vendor Report” (https://iapp.org/resources/article/2018-privacy-tech-vendor-report/)
169. Kinch, N. (3 April 2018) “Data Trust, by Design: Principles, Patterns and Practices (Part 2 – Up front Terms and Conditions” Medium.com (https://medium.com/greater-than-experience-design/data-trust-by-design-principles-patterns-and-practices-part-2-up-front-terms-and-conditions-337c6b37552d) and Kinch, N. (8 May 2018) “Data Trust, by Design: Principles, Patterns and Best Practices (Part 3 – Consent)” Medium.com (https://medium.com/greater-than-experience-design/data-trust-by-design-principles-patterns-and-best-practices-part-3-consent-70ccdb085f73)

Conclusion

Data collection, sharing and use practices are centrally important to our economic and social wellbeing as Australia enters the Fourth Industrial Revolution. Artificial Intelligence and machine learning technological developments promise massive benefits for the average Australian, but also risk entrenching and exasperating existing social and economic inequalities. Our data and personal information will be the fuel for these developments and consequently the rules we put in place to guide data collection, sharing and use will inform and influence the development of Artificial Intelligence processes and machine learning. Ensuring these practices are consistent with community expectations and work to enhance consumer welfare will be fundamental. We also, as a policy community, need to better understand how data is being used and the outcomes from that usage in order to enjoy the maximum benefits offered by these developments.

Policy and regulatory investigations around the world are concluding that data collection, sharing and use practices are resulting in substantial potential and actual consumer detriment. Many different approaches, grounded in competition, consumer protection, human rights and privacy perspectives, have been taken to respond to this problem. The first step will be to achieve transparency in the data collection sharing and use practices, along with building a better understanding of the supply chain. At present, consumers don't know what data is being collected about them or how it is being used. Regulators around the world are struggling to develop and apply models that adequately articulate how information and data markets work and design effective remedies that encourage ethical innovation while protecting consumer interests.

Failing to act now will risk exacerbating the lack of control and protections consumers already experience. Internationally, these concerns are already being acted upon – through investment in research and the implementation of new policies and regulations. It is time for Australia to bring our consumer markets into the 21st century by implementing a framework that both fosters good data practices and socially beneficial innovation.

References

Acxiom (2017) “2017 Annual Report”

Adobe Audience Finder (2019) “Epsilon” (https://www.adobe-audience-finder.com/data_partner/epsilon/)

Associated Press. (23 May 2017). “Google starts tracking offline shopping – what you buy at stores in person,” Los Angeles Times, (https://www.latimes.com/business/technology/la-fi-tn-google-ads-tracking-20170523-story.html)

Australian Competition and Consumer Commission (ACCC) (2018) Digital Platforms Inquiry: Preliminary Report (https://www.accc.gov.au/system/files/ACCC%20Digital%20Platforms%20Inquiry%20-%20Preliminary%20Report.pdf)

Bainbridge, A and Clark, E. (24 January 2019) “Insurers gaining ‘open-ended access’ to medical records slammed as ‘unfair privacy breach’” ABC News (https://www.abc.net.au/news/2019-01-24/medical-records-handed-to-insurance-companies-over-mental-health/10720024)

Batagol, B and Neave, M (1 February 2019) “Banks are Enabling Economic Abuse. Here’s How They Could Be Stopping It” The Conversation (https://theconversation.com/banks-are-enabling-economic-abuse-heres-how-they-could-be-stopping-it-110439)

Beilinson, J. (28 July 2016) “Glow Pregnancy App Exposed omen to Privacy Threats, Consumer Reports Finds” CR Consumer Reports (https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats/)

Belluz, J. (3 April 2018) “Grindr is revealing its users’ HIV status to third-party companies” Vox (https://www.vox.com/2018/4/2/17189078/grindr-hiv-status-data-sharing-privacy)

Benoliel, U. Becher, S. I. (11 January 2019) “The Duty to Read the Unreadable” 60 Boston College Law Review (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3313837)

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T. and Shadbolt, N. (27-30 May 2018) “Third party tracking in the mobile ecosystem” WebSci ’18, DOI https://doi.org/10.1145/3201064.3201089

Bradsher K. and Bennhold K. (23 January 2019) “World Leaders at Davos Call for Global Rules on Tech” The New York Times. (https://www.nytimes.com/2019/01/23/technology/world-economic-forum-data-controls.html)

Browne R. (24 January 2019) “Microsoft CEO says facial recognition technology needs to be regulated” CNBC.COM (https://www.cnbc.com/2019/01/24/davos-microsofts-nadella-says-facial-recognition-needs-regulation.html)

Business Wire (27 September 2018) “Visa and Oracle Introduce New Tools to Help Improve Digital Ad Performance” Business Wire (https://www.businesswire.com/news/home/20160927005676/en/Visa-Oracle-Introduce-New-Tools-Improve-Digital)

Calo, R. and Rosenblat, A. (9 March 2017) “The Taking Economy: Uber, Information, and Power” Columbia Law Review, Vol. 117, University of Washington School of Law Research paper No. 2017-18 (https://dx.doi.org/10.2139/ssrn.2929643)

Cardlytics (2019) “About us” (https://www.cardlytics.com/about-us/our-story/)

Cedarbaum, J G, Nahra, K J, and Freeman, Jr., D R (3 April 2019) “United States: Senate Subcommittee considers small business perspectives on a Federal Data Privacy Framework” Mondaq (http://www.mondaq.com/unitedstates/x/795444/Data+Protection+Privacy/Senate+Subcommittee+Considers+Small+Business+Perspectives+On+A+Federal+Data+Privacy+Framework)

Christl, W. (June 2017) “Corporate Surveillance in Everyday Life” Cracked Labs (https://crackedlabs.org/en/corporate-surveillance)

Christl, W. (October 2017) “How companies use personal data against people” Cracked Labs, p.23-25 (https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf)

Chung, F. (13 July 2016) “The Price You’re Paying for Loyalty,” News.com.au (https://www.news.com.au/finance/business/retail/the-price-youre-paying-for-loyalty/news-story/c6c2316fc3faef5dc86cd917c0cf729e)

Cliqz (14 May 2019) WhoTracks.me (htttps://whotracks.me)

CMO Staff (31 July 2015) “News Corp Partners with Quantium and MCN to Launch New Digital Advertising Products,” CMO, (https://www.cmo.com.au/article/580909/news-corp-partners-quantium-mcn-launch-new-digital-advertising-products/)

Culnane,C., Rubinstein, B. I. P. and Teague, V. (December 2017) “Health Data in an Open World” (https://arxiv.org/ftp/arxiv/papers/1712/1712.05627.pdf)

Danova, T. (21 June 2014) “Bricks-And-Mortar Retailers Will Use Beacons to Combat The Showrooming Threat,” Business Insider Australia, (https://www.businessinsider.com.au/bricks-and-mortar-retailers-will-use-beacons-to-combat-the-showrooming-threat-2014-6)

Day, M, Turner, G, and Drozdiak, N (11 April 2019) “Amazon workers are listening to what you tell Alexa” Bloomberg (https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio)

De Mooy, M. (7 August 2017) “Hotspot Shield VPN’s Privacy and Security Promises Contradict Practices. Centre for Democracy and Technology” CDT.org (https://cdt.org/blog/hotspot-shield-vpns-privacy-and-security-promises-contradict-practices/)

de Montjoye, Y. A., Hidalgo, C.A., Verleysen, M. and Blondel, V.D. (25 March 2013) “Unique in the Crowd: The Privacy Bounds of Human Mobility,” Scientific Reports 3, Article Number: 1376 (https://www.nature.com/articles/srep01376)

Dent, J. (22 February 2019) “When can you get 5G in Australia?” WhistleOut (https://www.whistleout.com.au/MobilePhones/Guides/when-can-you-get-5G-in-Australia)

Department for Digital, Culture, Media and Sport (20 November 2018) “Consultation outcome. Centre for Data Ethics and Innovation Consultation.” (https://www.gov.uk/government/consultations/consultation-on-the-centre-for-data-ethics-and-innovation/centre-for-data-ethics-and-innovation-consultation#the-centres-role-and-objectives

Dubbeldam, B. (11 January 2019) “Principles of ‘Good Data’” Network Cultures (http://networkcultures.org/blog/2019/01/11/principles-of-good-data/)

Duhaime-Ross, A. (19 September 2014) “Here’s how well Google’s search engine knows you” The Verge (https://www.theverge.com/2014/9/19/6409773/heres-how-well-googles-search-engine-knows-you)

Easton, S. (19 July 2018) “Cass Sunstein’s Bill of Rights for Nudging” The Mandarin (https://www.themandarin.com.au/96009-cass-sunsteins-bill-of-rights-for-nudging/)

Editorial Board (2 February 2019) “How Silicon Valley Puts the ‘Con’ in Consent,” The New York Times, (https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html)

Epsilon (2019) “Case Study Norwegian Cruise Line” (https://us.epsilon.com/award-winning-marketing-case-studies/ncl)

Epsilon (2019) “Our Industry-Leading Experts are Ready to Grow Your Business” Epsilon website (https://emea.epsilon.com/data-driven-personalised-marketing-services#one)

Epsilon (2019) “What We Do Data” Epsilon website (https://emea.epsilon.com/data-driven-marketing-solutions/people-based-marketing-data-solution)

Epsilon (2019) “Who We Are Our Partners” Epsilon website (https://apac.epsilon.com/people-based-marketing-solutions-epsilon/data-driven-marketing-solutions-partners)

European Commission (14 February 2019) “Digital Single Market: EU negotiators agree to set up new European rules to improve fairness of online platforms’ trading practices” European Commission (http://europa.eu/rapid/press-release_IP-19-1168_en.htm)

Experian (undated) “Discover Experian 2016” Annual Report (https://www.experianplc.com/media/2744/discover-experian-fy17.pdf)

Experian (2019) “Partnerships and integrations” (https://www.edq.com/partners/)

Experian (2019) “The Data We Obtain” (http://www.experian.com.au/consumer-information-portal/about-our-data)

Farrell, P., Ting, I., and Donaldson, A. (15 March 2019) “Sportsbet’s big punt,” ABC News, (https://www.abc.net.au/news/2019-03-05/sportsbet-documents-reveal-millions-spent-on-marketing/10833196)

Federal Trade Commission (May 2014) Data Brokers: A Call for Transparency and Accountability (https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf)

Fergus, R. (21 March 2019) “Data sharing by popular health apps is ‘routine’, research finds” The University of Sydney (https://sydney.edu.au/news-opinion/news/2019/03/21/data-sharing-by-popular-health-apps-is--routine---research-finds.html)

Fitbit website (2019) “Versa” (https://www.fitbit.com/au/versa)

Foster, J.B. and McChesney, R. W. (2014) “Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age” Monthly Review (https://monthlyreview.org/2014/07/01/surveillance-capitalism/)

Fowler, G. A. (31 January 2019) “The Doorbells Have Eyes: The Privacy Battle Brewing Over Home Security Cameras” The Washington Post (https://www.washingtonpost.com/technology/2019/01/31/doorbells-have-eyes-privacy-battle-brewing-over-home-security-cameras/?utm_term=.de9ff39e42e4)

Frischmann, B. (19 February 2019) “Electronic Contracts and the Illusion of Consent” Scientific American (https://blogs.scientificamerican.com/observations/electronic-contracts-and-the-illusion-of-consent/)

Greenberg, A (27 June 2018) “Marketing firm Exactis leaked a personal info database with 340 million records” Wired (https://www.wired.com/story/exactis-database-leak-340-million-records/)

Grothaus, M. (3 january 2019) “5G means you’ll have to say goodbye to your location privacy” Fast Company (https://www.fastcompany.com/90314058/5g-means-youll-have-to-say-goodbye-to-your-location-privacy)

Grundy, Q. (20 March 2019) “Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis” BMJ (https://www.bmj.com/content/364/bmj.l920)

Guess, M. (22 July 2016) “PayPal Will Share Data, Plug Visa in Exchance for Wider Terminal Acceptance” ArsTechnica (https://arstechnica.com/information-technology/2016/07/paypal-will-share-data-plug-visa-in-exchange-for-wider-terminal-acceptance/)

Hanley, G (15 December 2017) “If you go down to the mall today, you’re watched by a thousand eyes” The Sydney Morning Herald (https://www.smh.com.au/technology/if-you-go-down-to-the-mall-today-youre-watched-by-a-thousand-eyes-20171211-h02h9q.html

Harari, Y.N. (2018) Twenty-one lessons for the Twenty-First Century, UK: Penguin Random House

Harwell, D. (10 April 2019) “Is Your Pregnancy App Sharing Your Intimate Data With Your Boss?” The Washington Post (https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/?utm_term=.e3825c86adb3)

Hayne, K (4 March 2019) “Kenneth Hayne’s final royal commission report held back ‘heavy hits’ from the banks” ABC News (https://www.abc.net.au/news/2019-02-26/hayne-banking-royal-commission-squib/10832620)

Heller, N. (26 February 2019) “Why the Life-Insurance Industry Wants to Creep on Your Instagram” New Yorker (https://www.newyorker.com/culture/cultural-comment/why-the-life-insurance-industry-wants-to-creep-on-your-instagram)

Hemingway Editor (2015) “Help” (http://www.hemingwayapp.com/help.html)

Hill, K. (16 February 2012) “How Target Figured Out a Teen Girl was Pregnant Before Her Father Did” Forbes (https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#43a8159c6668)

International Association of Privacy Professionals (2019) “2018 Privacy Tech Vendor Report” (https://iapp.org/resources/article/2018-privacy-tech-vendor-report/)

Isaac, M. (23 April 2017) “Uber’s CEO Plays With Fire” The New York Times (https://www.nytimes.com/2017/04/23/technology/travis-kalanick-pushes-uber-and-himself-to-the-precipice.html)

Kemp, K. (27 September 2018) “Getting Data Right” Center for Financial Inclusion (https://www.centerforfinancialinclusion.org/getting-data-right)

Kinch, N. (3 April 2018) “Data Trust, by Design: Principles, Patterns and Practices (Part 2 – Up front Terms and Conditions” Medium.com (https://medium.com/greater-than-experience-design/data-trust-by-design-principles-patterns-and-practices-part-2-up-front-terms-and-conditions-337c6b37552d) and Kinch, N. (8 May 2018) “Data Trust, by Design: Principles, Patterns and Best Practices (Part 3 – Consent)” Medium.com (https://medium.com/greater-than-experience-design/data-trust-by-design-principles-patterns-and-best-practices-part-3-consent-70ccdb085f73)

Koebler, J (13 November 2018) “The weakest link in cybersecurity isn’t human, it’s the infrastructure” Motherboard VICE (https://www.vice.com/en_us/article/d3bvgy/the-weakest-link-in-cybersecurity-isnt-human-its-the-infrastructure)

Koren, J R (19 December 2015) “Some lenders are judging you on much more than your finances” Los Angeles Times (https://www.latimes.com/business/la-fi-new-credit-score-20151220-story.html)

Lecher, C. (12 December 2018). “Democratic senators have introduced a big new data privacy plan” The Verge (https://www.theverge.com/2018/12/12/18138131/democratic-data-care-act-senate-law)

LinkedIn (2019) “LinkedIn in Microsoft Applications with Your Personal Account” https://www.linkedin.com/help/linkedin/answer/84711/linkedin-in-microsoft-applications-with-your-personal-account?lang=en

Maheshwari, S. (5 July 2018) “How Smart TVs in Millions of U.S. Homes Track More Than What’s On Tonight” The New York Times (https://www.nytimes.com/2018/07/05/business/media/tv-viewer-tracking.html)

Mann, M., Devitt, K. and Daly, A. (2019) “What Is (In) Good Data” In Daly, A., Devitt, K., and Mann, M. (Eds.) Good Data Amsterdam: Institute of Network Cultures (https://eprints.qut.edu.au/123773/)

Manokha, I. 2018, “Surveillance: The DNA of Platform Capital—The Case of Cambridge Analytica Put into Perspective”, Theory & Event, Volume 21, Number 4, October 2018, p. 895 (chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://ora.ox.ac.uk/objects/uuid:15e74c10-225f-4bd7-b0868e1fdb1b79e8/download_file?file_format=pdf&safe_filename=Manokha%252C%2BSurveillance%252C%2BAAM.pdf&type_of_work=Journal+article)

Manwaring, K. (2017) “Will emerging technologies outpace consumer protection law? The case of digital consumer manipulation” Competition & Consumer Law Journal, 26

Marechal, N. (17 November 2018) “Targeted Advertising is Ruining the Internet and Breaking the World” Motherboard (https://motherboard.vice.com/en_us/article/xwjden/targeted-advertising-is-ruining-the-internet-and-breaking-the-world)

MindBodyOnline (31 December 2018) “How We Collect Information” (https://www.mindbodyonline.com/privacy-policy)

Mitchell, S. (4 October 2018) “Woolworths Hands Data Sharing Contracts to Quantium, Nielsen,” Australian Financial Review (https://www.afr.com/business/retail/woolworths-hands-data-sharing-contracts-to-quantium-nielsen-20181004-h16819)

National Australia Bank (3 August 2017) “NAB Online Retail Sales Index: Indepth Report – June 2017” (https://business.nab.com.au/nab-online-retail-sales-index-indepth-report-june-2017-25397/)

Naughton, J. “‘The goal is to automate us’: welcome to the age of surveillance capitalism,” The Guardian, (https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook)

New Mexico Attorney General (12 September 2018) “AG Balderas Announces Lawsuit Against Tech Giants Who Illegally Monitor Child Location, Personal Data” Presse Release (https://www.nmag.gov/uploads/PressRelease/48737699ae174b30ac51a7eb286e661f/AG_Balderas_Announces_Lawsuit_Against_Tech_Giants_Who_Illegally_Monitor_Child_Location__Personal_Data_1.pdf)

Nguyen P. and Solomon L. (2018) Consumer Data and the Digital Economy, Melbourne: Consumer Policy Research Centre (http://cprc.org.au/2018/07/15/report-consumer-data-digital-economy/)

Nikkei Asian Review (24 February 2017) “Japan takes step toward enormous bank of personal data” (https://asia.nikkei.com/Economy/Japan-takes-step-toward-enormous-bank-of-personal-data)

Nine Entertainment Co. Privacy Policy (Undated) (https://login.nine.com.au/privacy?client_id=9nowweb)

Nine Entertainment Co. (2018) “Data & Targeting” (https://www.nineentertainmentco.com.au/brand-data)

Norwegian Consumer Council (27 June 2018) Deceived by Design, p.39 (https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf)

OECD (2013) “Exploring the economics of personal data: A Survey of Methodologies for Measuring Monetary Value” OECD Digital Economy Papers. No. 220. Paris: OECD Publishing (https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en)

OECD Digital Economy Papers (January 2019) “Vectors of Digital Transformation” (https://www.oecd-ilibrary.org/science-and-technology/vectors-of-digital-transformation_5ade2bba-en)

O’Neil, C. (2016) Weapons of Math Destruction USA: Crown Books

Osborne, C. (21 February 2019) “Google says ‘hidden’ microphone in Nest product never intended to be a secret” Zero Day in ZDNet (https://www.zdnet.com/article/google-says-secret-microphones-in-nest-home-products-an-error/)

Ovide, S. (6 April 2018) “Private Messages Aren’t Exactly Private at Facebook” Bloomberg (https://www.bloomberg.com/opinion/articles/2018-04-05/facebook-private-messages-aren-t-exactly-private)

Parker C. (24 January 2019) “Privacy is a human right, we need a GDPR for the world: Microsoft CEO” World Economic Forum (https://www.weforum.org/agenda/2019/01/privacy-is-a-human-right-we-need-a-gdpr-for-the-world-microsoft-ceo/)

Privacy by Design Centre of Excellence (Undated) “The Seven Foundational Principles” Ryerson University (https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/)

Quantium website, accessed 3 April 2019, (https://www.quantium.com/)

Razaghpanah, A. Nithyanand, R. Vallina-Rodriguez, N. Sundaresan, S. Allman, M. Kreibich, C. and Gill, P. (18-21 February 2018) “Apps, Trackers, Privacy and Regulators. A Global Study of the Mobile Tracking Ecosystem,” Conference paper, Proceedings of Network and Distributed Systems Security (NDSS) Symposium 2018, (http://eprints.networks.imdea.org/1744/)

Reyes, I, Wijesekera, P, Reardon, J, Bar On, A E, Razaghpanah, A, Vallina-Rodriguez, N and Egelman, S. (2018) "'Won't Somebody Think of the Children?' Examining COPPA Compliance at Scale" Proceedings on Privacy Enhancing Technologies, pp.63-83 (https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf)

(undated) "Rights Related to Automated Decision Making Including Profiling" Information Commissioner's Office (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/)

Rohrer, C (12 October 2014) "When to use which user-experience research methods" NN/g Nielsen Norman Group (https://www.nngroup.com/articles/which-ux-research-methods/)

Ross, A. "How Big Tech Built the Iron Cage," New Yorker, (https://www.newyorker.com/culture/cultural-comment/building-the-digital-iron-cage)

Schechner, S (22 February 2019) "You give apps sensitive personal information. Then they tell Facebook." Outline (https://www.outline.com/w5w5RP)

Serrrato, J. K., Cwalina, C., Rudawski, A., Coughlin, T. and Fardelmann, K. (9 July 2018) "US states pass data protection laws on the heels of the GDPR" Norton Rose Fulbright (https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/)

Singer, N. (16 June 2012) "Mapping, and Sharing, the Consumer Genome," The New York Times (https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html)

Sloane, G. (28 March 2018) "Facebook Turns Off Ad Targeting Tool Based on Third-Party Data," AdAge, (https://adage.com/article/digital/facebook-turns-targeting-tool-based-party-data/312912/)

Snapchat privacy policy (1 October 2018) (https://www.snap.com/en-US/privacy/privacy-policy/)

Solon, O. (12 March 2019) "Facial recognition's 'dirty little secret': Millions of online photos scraped without consent" NBC News (https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921)

Spielkamp, M. (12 June 2017) "Inspecting algorithms for bias" MIT Technology Review (https://www.technologyreview.com/s/607955/inspecting-algorithms-for-bias/)

Stewart, R. (18 July 2018) "Snapchat Extends Nielsen Deal So Brands Can Target Shoppers Based on Offline Data" (https://www.thedrum.com/news/2018/07/18/snapchat-extends-nielsen-deal-so-brands-can-target-shoppers-based-offline-data)

Street, F. (3 March 2019) "Can airplane seat cameras spy on passengers?" CNN Travel https://edition.cnn.com/travel/article/airplane-seat-camera-intl/index.html

Sweney, M. (13 March 2019) "Hammond calls for regulator to investigate UK's digital ads market" The Guardian (https://www.theguardian.com/media/2019/mar/13/hammond-calls-for-regulator-investigation-uk-digital-ad-market-facebook-google)

Tische, M. (14 December 2018) "It's Time for a Bill of Data Rights" MIT Technology Review (https://www.technologyreview.com/s/612588/its-time-for-a-bill-of-data-rights/)

Turow, J. Hennessy, M. and Draper, N. (2015) "The Tradeoff Fallacy: How Marketers and Misrepresenting American Consumers and Opening Them Up to Exploitation" SSRN Electronic Journal, 10.2139/ssrn.2820060

UK Government (2019) "Unlocking Digital Competition" (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf)

Van Dorpe, S (7 February 2019) "German competition authority orders Facebook to change data collection procedures" Politico (https://www.politico.eu/article/german-competition-authority-orders-facebook-to-change-data-collection-procedures/)

Valentino-DeVries, J., Singer, N., Keller, M.H. and Krolik, A. (10 December 2018) "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," The New York Times. (https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html)

Visa Global Privacy Notice (23 May 2018) (https://www.visa.com.au/legal/global-privacy-notice.html)

Vlahos, J. (26 March 2019) "Smart Talking: Are Our Devices Threatening Our Privacy" The Guardian (https://www.theguardian.com/technology/2019/mar/26/smart-talking-are-our-devices-threatening-our-privacy)

Vocational Literacy (undated) "ABS Research: 46% of Australians Adults Aged 16-70 are Illiterate" (http://vocationalliteracy.com.au/research-into-adult-literacy-in-australia/)

Wallbank, P (29 March 2019) "Facebook shuts down third-party advertiser access in wake of Cambridge Analytica scandal" Mumbrella https://mumbrella.com.au/facebook-shuts-third-party-advertiser-access-wake-cambridge-analytica-scandal-508085

Whigham, N. and Associated Press (14 August 2018) "Google will keep tracking your every movement, like it or not" News.com.au (https://www.news.com.au/technology/gadgets/mobile-phones/google-will-keep-tracking-your-every-movement-like-it-or-not/news-story/7f6daa18cbe444cc11e2b1360e63f857)

Whittaker, Z. (2019) "Many popular iPhone apps secretly record your screen without asking" TechCrunch (https://techcrunch.com/2019/02/06/iphone-session-replay-screenshots/)

Whotracks.me website (2019) (https://whotracks.me/)

Woolworths (4 October 2018) "Announcement from Peter and Paul" (http://www.wowlink.com.au/cmgt/wcm/connect/345dfe80473b4826a32ca35fa1287528/Update+on+Woolworths+Data+Sharing+RFP.pdf?MOD=AJPERES)

Woolworths Group Privacy Policy (January 2018) (https://www.woolworthsgroup.com.au/page/privacy-policy/)

Woolworths Rewards Privacy Policy (6 June 2018) (https://www.woolworthsrewards.com.au/privacy.html)

Zuboff, S. (2019) The Age of Surveillance Capitalism, New York: Hatchette Book Group

Zuiderveen Borgesius, F. (2018) "Discrimination, artificial intelligence, and algorithmic decision-making" Council of Europe, p.21 (https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73)

Appendices

Appendix 1: Experiment methodology

Experiment design

Landscape of user research methods (Graph A)

A variety of user research methods exist to help researchers ask and answer research questions with appropriate confidence intervals. This diagram, inspired by Christian Rohrer's 2014 work for NNG Group, showcases 20 popular user research methods. It visualises them using a three dimensional framework that covers:

1. Attitudinal vs Behavioural,
2. Qualitative vs Quantitative, and
3. Context of use.

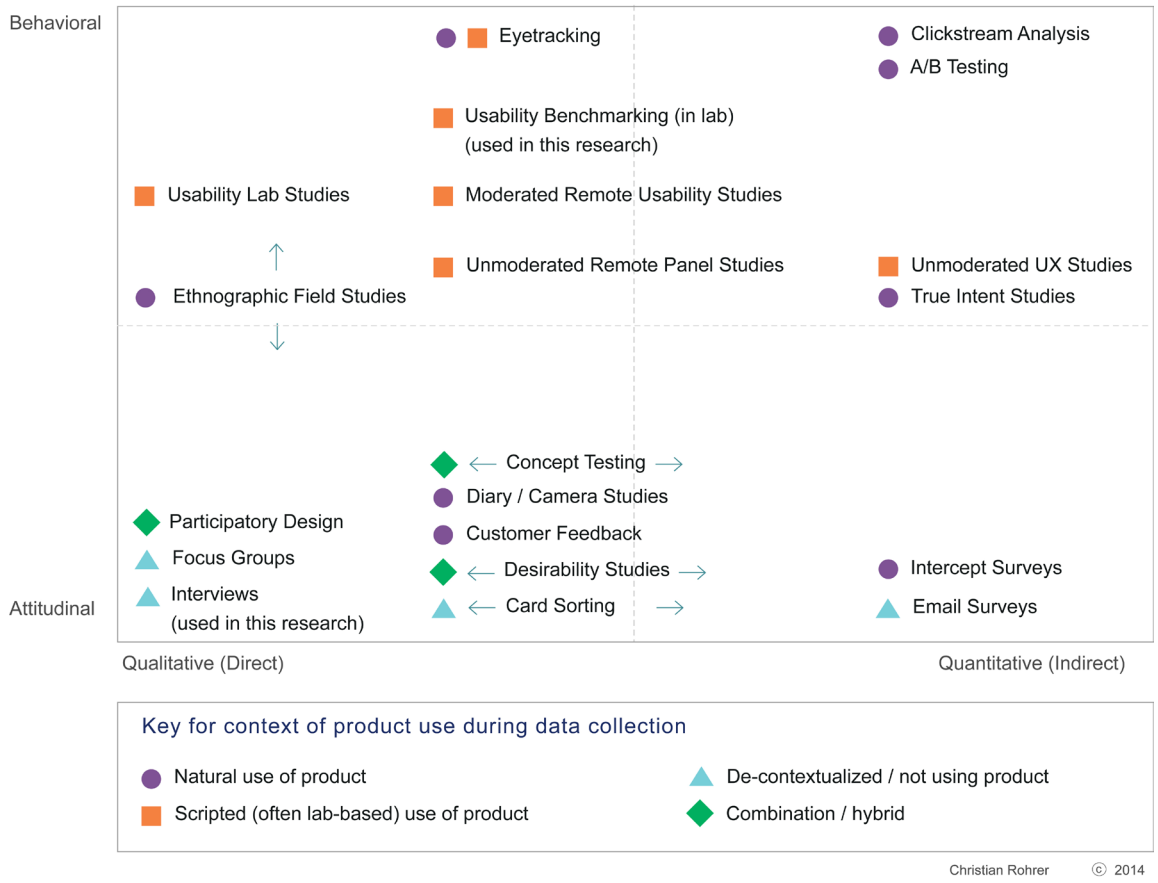
The participants were not performing a live internet search. Greater Than X created a clickable prototype that mimicked the experience of searching, purchasing and paying online. The experience of the search, purchase, and payment process was designed to reflect the common practices used in data collection and processing. The actual privacy policies and terms and conditions were used for the following services mimicked in the experiment: PayPal, Apple and Google. The site at the time of testing, apart from the cruise website's privacy policy and terms and conditions which was modified from similar agreements.

Questions answered (Graph B)

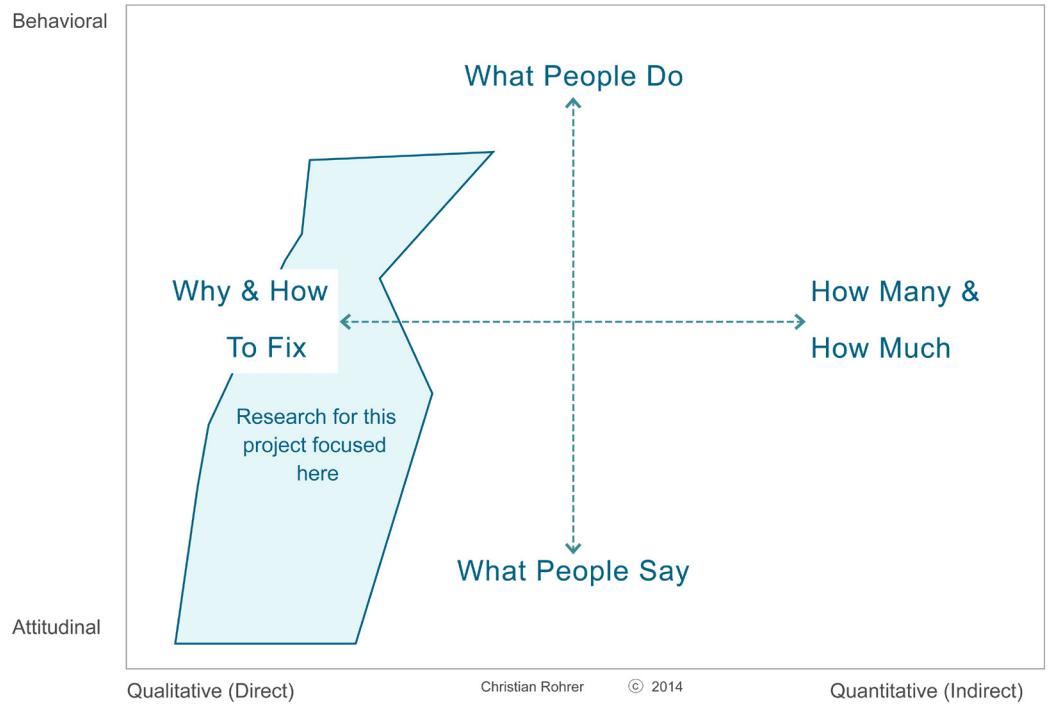
Based on project constraints, along with the research questions Greater Than X asked and the answers they aimed to discover, they focused largely on qualitative research across the attitudinal dimension. Greater Than X added a specific, simulated situational context to each research session to help develop a 'proxy' understanding for the behaviours people exhibit when signing up to products and services and engaging with a variety of agreements, like Terms and Conditions and Privacy Notices.

This helped to develop a foundational understanding of how people feel about existing agreements. It also helped to begin deepening an understanding of how people actually behave when faced with such agreements.

Graph A: A Landscape of User Research Methods



Graph B: Questions Answered by Research Methods Across the Landscape



Experiment Context

The research involved consumer interviews using contextual inquiry and usability methodologies with a clickable prototype that was designed to reflect the common practices used in data collection and processing. A market research firm was engaged to recruit participants based on the following characteristics:

Demographic

Gender: F

Age: 28-40

Education: High-school minimum

Employment: PT/Casual

Relationship status: married with dependents (kids)

Geographic

Residential: Sydney

Behavioural

Browsing Behaviour: Browses more than 4-5 times a month

Purchasing Behaviour: Purchased something online within the last month

Shops online: 1-2 times per week

On-demand TV: 2-3 times per week

The criteria was based on a few assumptions.

- Gender was set as female as the day in the life activities outline was reflective of a female.
- A specified gender also allowed for expediency in recruiting participants as we had a one week timeframe.
- The focus on females allowed the research to limit variability of participant characteristics.
- Behavioural characteristics were chosen to align as closely as possible to the generalised activities defined in an average day of an Australian consumer.

The research sessions with participants were conducted using a laptop connected to a large screen display to observe participant interactions. Although the prototype was on mobile, this form factor was chosen to reduce issues with network connectivity and enable session room screen display. Prior to commencement, consent to record audio and video interactions on screen was acquired to allow for more detailed analysis. The participants' behaviour and reactions during the research sessions were observed and recorded by a note taker.

In analysing and aggregating the data gathered, a spreadsheet was formatted with specified fields as follows:

- The screen presented
- Participant responses from research session
- Participants' observed behaviour
- Key words
- Emergent themes
- Inferred Behavioural State

Participants were presented with a mobile experience where they are purchasing a gift for Valentine's day. The mobile experience is not a real app or website but participants were able to interact with it as normal. A script is used for guiding questions for the researcher. When participants go to specific screens these guiding questions enable the research to inquire further and engage in exploratory queries into the feelings, attitudes and sentiments of the participants.

To simulate the experience, participants were given context for the experiment:

> "You've been on the hunt for the perfect Valentine's Day surprise for a while now. You have successfully convinced your partner that there is absolutely nothing being planned but really, you've been actively researching on-and-off for the last 3 weeks. After much consideration, you have decided on a romantic cruise dinner on the Sydney Harbour. However, you can't remember exactly which cruise company impressed you the most. To locate and purchase from the cruise company in your memory, you search "valentine's day" on Google."

Participants went through the search, purchase and payment process as normal. Their behaviour was observed by researchers. They then went through the process a second time with researchers asking questions at each screen. Finally, the researchers led a discussion about data collection practices with each participant.

Experiment Process/Questions

1. Google Search “Valentine’s Day”. Search history is shown as the person types in Valentine’s Day.
2. Top recommendation is already a previously visited website for a cruise experience.

    a. How do you feel about previously visited searches and websites being shown as the top search result?

    b. Follow Up: How would you feel if you had searched something general, like "things to do Sydney" and the same results popped up?
3. “Update to Privacy Policy and How We Use Cookies” covers half of the screen. “Accept” and “View Details” is the only given choice.

    a. How does the Privacy Policy update covering half of the screen make you feel?

    b. Do you feel that you have a choice to say “No” here?
4. The User clicks “view details” which pulls up a page full of text that is of readability level 11. //prompt the participant to skim read “I want you to have a go at reading the legal agreement”

    a. What is your initial impression of their Terms and Conditions?

    b. When you read the Terms and Conditions, do you feel that you understood the contract you are agreeing to?
5. Clicks accept and is immediately shown ads at the bottom of the screen from Retailer 2 whose site was previously visited.

    a. How do the ads make you feel?
6. Views the event, Clicks through to select a time.
7. Selects 2 standard tickets at $130 per ticket. Another ad is shown from Retailer 3.
8. Delivery Options shown. Below there is a notice in very small font “By clicking through, you are agreeing to our Terms of Service”

    a. Did you notice the requirement for your agreement to their ToS?

    b. Do you feel that you were well informed about the contract that is being put forward?
9. User is required to sign in, create an account or “Continue as a guest”.

    a. What is your preference here? Why?
10. Every field of “Your Details” are required for user to make a purchase.

    a. How do you feel about sharing all this information?

11. User given options of PayPal or Credit Card. Credit Card has Mastercard, Visa or Debit options. User inputs credit card details and clicks through to “Place Order”. Below there is a notice in very small font “By clicking through, you are agreeing to our Privacy Policy”

    a. Did you notice the requirement for your agreement to their Privacy Policy?

    b. Do you feel that you understand how they will use your personal information?

12. User chooses PayPal option. User redirected to PayPal site to login. User is able to log in with a saved password.

    a. If user clicks through to- Privacy Notice: This takes 19 minutes of reading time… how does that make you feel?

    b. Terms of Service: This takes 20 minutes of reading time and that is only one of the eight sections in the Paypal T&Cs… how does that make you feel?

13. User’s preferred card is already selected by PayPal. User able to click through for more information on card / their transaction history.

14. PayPal is marked with a tick to indicate selection. User clicks through to “Place Order”. Below there is a notice in very small font “By clicking through, you are agreeing to our Privacy Policy”

15. Order Summary Shown - “Welcome Aboard!” Catch Phrase. Notification from Maker “We have found an event of the 14 February, 2019. Would you like to add to calendar?” User

16. Clicks “Yes, Add”.

    a. How did you feel about Apple’s recognition of this event for you?

Level 14, 10-16
Queen Street

Melbourne
Victoria 3000

T 03 9639 7600
F 03 9639 8966

cprc.org.au
ACN 100 188 752

Consumer
Policy Research
Centre