

Devil in the detail

Privacy and some popular digital platforms

Popular digital platforms use privacy policies and terms & conditions documents that are long, complicated and contain worrying provisions. Users cannot give informed consent to terms & conditions that they do not understand. Reform is needed to protect users and guarantee that consent is informed.

Discussion paper

Agatha Court

Bill Browne

December 2020

About The Australia Institute

The Australia Institute is an independent public policy think tank based in Canberra. It is funded by donations from philanthropic trusts and individuals and commissioned research. We barrack for ideas, not political parties or candidates. Since its launch in 1994, the Institute has carried out highly influential research on a broad range of economic, social and environmental issues.

About the Centre for Responsible Technology

The Australia Institute established the Centre for Responsible Technology to give people greater influence over the way technology is rapidly changing our world. The Centre will collaborate with academics, activists, civil society and business to shape policy and practice around network technology by raising public awareness about the broader impacts and implications of data-driven change and advocating policies that promote the common good.

Our philosophy

As we begin the 21st century, new dilemmas confront our society and our planet. Unprecedented levels of consumption co-exist with extreme poverty. Through new technology we are more connected than we have ever been, yet civic engagement is declining. Environmental neglect continues despite heightened ecological awareness. A better balance is urgently needed.

The Australia Institute's directors, staff and supporters represent a broad range of views and priorities. What unites us is a belief that through a combination of research and creativity we can promote new solutions and ways of thinking.

Our purpose—'Research that matters'

The Institute publishes research that contributes to a more just, sustainable and peaceful society. Our goal is to gather, interpret and communicate evidence in order to both diagnose the problems we face and propose new solutions to tackle them.

The Institute is wholly independent and not affiliated with any other organisation. Donations to its Research Fund are tax deductible for the donor. Anyone wishing to donate can do so via the website at <https://www.tai.org.au> or by calling the Institute on 02 6130 0530. Our secure and user-friendly website allows donors to make either one-off or regular monthly donations and we encourage everyone who can to donate in this way as it assists our research in the most significant manner.

Level 1, Endeavour House, 1 Franklin St
Canberra, ACT 2601
Tel: (02) 61300530
Email: mail@tai.org.au
Website: www.tai.org.au
ISSN: 1836-9014

Summary

The collection of user data by digital platforms is ubiquitous. This user information is a valuable resource—in 2017, the global value of the data economy was estimated to be US\$3 trillion.

Data collection is not just the result of users' direct interactions with digital platforms but also the result of data collected indirectly from third parties and public sources.

User data collection is enabled by the terms and conditions and privacy policies of digital platforms, to which users must agree to be able to use their services. These policies are long and complex legal contracts and, as a result, most users neither fully read them nor understand their consequences—they therefore agree to them without informed consent.

This report examines the terms and conditions and privacy policies of some popular digital platforms (Qantas Frequent Flyer, NAB, MyFitnessPal, Westfield WiFi and Woolworths Rewards) and demonstrates their length and complexity and concerning terms they contain. In doing so, it raises the question whether stricter rules governing permitted terms in contracts for digital platforms and stronger privacy laws are necessary.

Introduction

Most Australians use a website or app everyday—to shop, stream videos, read the news, talk to friends, use transport or access their bank account. In fact, it is almost impossible to interact with the modern world without using online platforms.

The websites and apps (digital platforms) that we use have terms and conditions for their use and most also have separate privacy policies. These are legal contracts and they are long and full of legal jargon. Most people do not read them—they simply click “accept” and go about their day. But, in doing so, users are signing away their right to privacy because of terms and conditions that grant these digital platforms extraordinary access to their personal information.

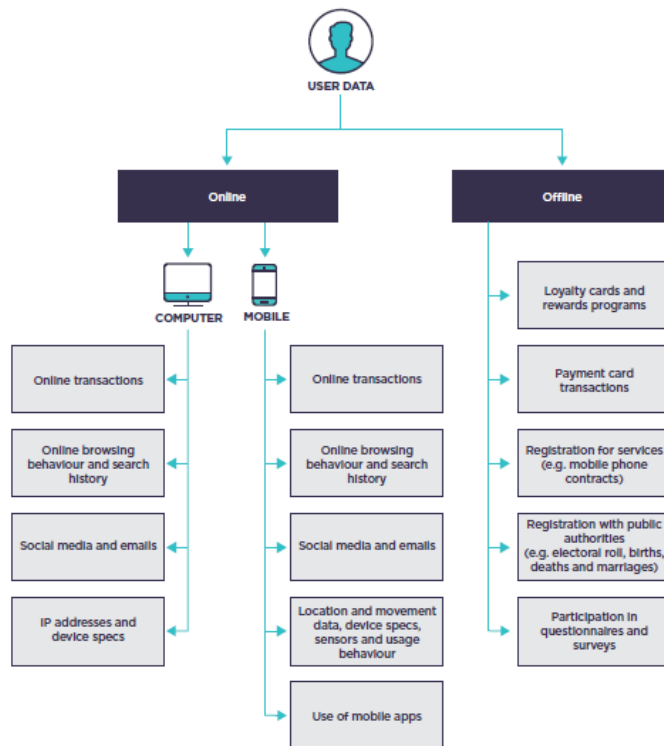
Much has been written about the data mining habits of the big social media platforms and search engines like Facebook and Google (including recently by the Australian Competition and Consumer Commission (ACCC) in its Digital Platforms Inquiry).¹ Their business model relies on their ability to extensively track users' likes and preferences for the purpose of advertising. Yet it is not just these big players that do this—user surveillance is present across the digital economy.

Digital platforms collect significant user data. They do this in three main ways. Firstly, they collect the data the user actively provides, such as their name and email, when signing up for a platform. Secondly, data, such as the user's IP address, location and use of third-party websites, is passively collected. And, lastly, inferred data is created when platforms analyse users' active and passive data to create an extensive picture of a user's habits.²

¹ ACCC (2019) *Digital Platforms Inquiry: Final Report*, <https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report>

² ACCC (2019) *Digital Platforms Inquiry: Final Report*, pp. 377–378

Figure 1: Tracking users' data online and offline



Source: ACCC (2019) *Digital Platforms Inquiry: Final report*, p. 378,
<https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report>

User information is a valuable resource. In 2017, the global value of the data economy was estimated to be US\$3 trillion.³ User data, such as likes and dislikes, friends, spending habits, search history and location, is so valuable because of the sheer volume that tech platforms collect. According to multiple estimates, 90 per cent of the data that exists has been compiled in the past two years.⁴ As large digital platforms have near-monopoly status and because they own numerous other online services, they are able to collect different types of data and share it amongst themselves. For example, Google has 60 different online services that collect and combine data to form a highly detailed profile of an individual.⁵

The digital world is difficult for individual users to navigate. Government regulation is outdated and leaves the navigation up to the individual who is legally envisaged as an expert on privacy and contract law. However, the reality is that the average user neither reads the terms and conditions nor understands their consequences.

³ Thirani & Gupta (2017) *The value of data*, <https://www.weforum.org/agenda/2017/09/the-value-of-data/>

⁴ Dipple-Johnstone (2018) *Beesley Lecture - 'Regulating the tech giants in the digital age,'*
<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/beesley-lecture-regulating-the-tech-giants-in-the-digital-age/>

⁵ ACCC (2019) *Digital Platforms Inquiry: Final report*, p. 379

An ACCC consumer survey found that 60 per cent of Australians rarely or never read the terms and conditions of digital platforms before accepting them.⁶ The ACCC also found that almost all of the privacy policies of the major digital platforms it reviewed required a university education to understand.⁷ However, these terms and conditions and privacy policies are legally binding contracts and, by accepting them, users are giving digital platforms enormous access to their personal information.

To illustrate the difficulty users face in having the time to read and understand these policies, this report investigates the terms and conditions and privacy policies of some popular websites and apps—Qantas Frequent Flyer, NAB, MyFitnessPal, Westfield WiFi and Woolworths Rewards. The report demonstrates the length and complexity of these policies as well as some concerning terms contained within the conditions.

⁶ ACCC (2019) *Digital Platforms Inquiry: Final Report*, p. 396

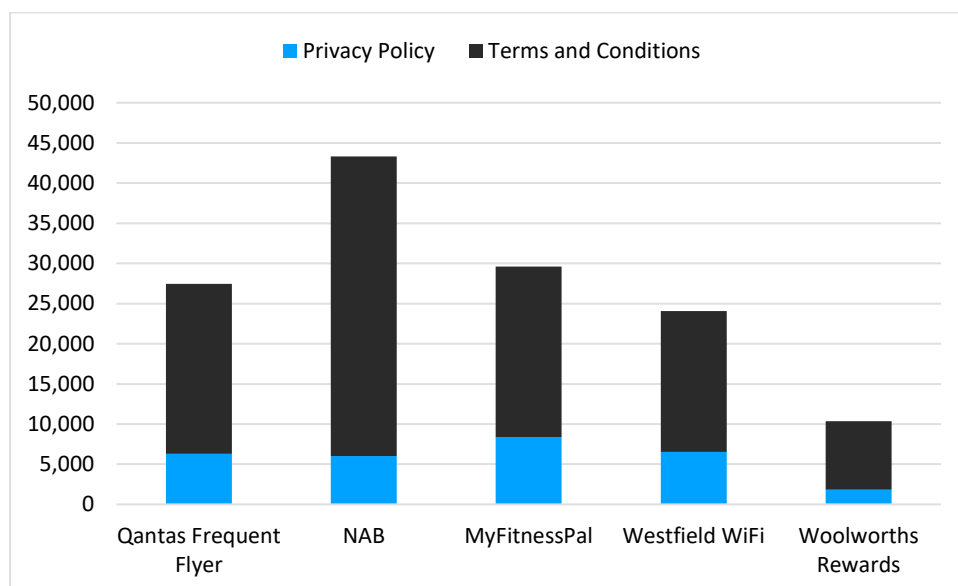
⁷ ACCC (2019) *Digital Platforms Inquiry: Final Report*, p. 405

Length and readability of documents

How long would it take to read the terms and conditions and privacy policies of our chosen platforms? Even if you had that time on your hands, would you be able to understand these documents?

Figure 2 below summarises the word count of the privacy policies and terms and conditions of the digital platforms examined. The terms and conditions for NAB and Qantas are especially large because they include the terms for several different products within the same document. Separate Cookies policies are not included.

Figure 2: Word count of privacy policies and terms and conditions



Source: Author's calculations based on source documents

Table 1 below summarises the length of these documents, estimated reading time and an assessment of their readability using the Flesch Reading Ease Formula (also used by the ACCC in its inquiry). This Formula produces a score from 0 to 100 with the higher the score for a document indicating that it is easier to read. For example, a score from 0 to 30 indicates a document is very difficult to read, being the expected reading level of a university graduate level, while a score of 30 to 50 indicates it is difficult to read, an expected reading level of a university student.⁸

⁸ Flesch (n.d.) *How to Write Plain English*, chap. 2,

https://web.archive.org/web/20160712094308/http://www.mang.canterbury.ac.nz/writing_guide/writing/flesch.shtml. The full formula is $\text{Readability Ease} = 206.835 - (1.015 \times \text{Average Sentence Length}) - (84.6 \times \text{Average Number of Syllables Per Word})$ See: *Readability Formulas* (n.d.) *The Flesch Reading Ease Readability Formula*, <https://readabilityformulas.com/flesch-reading-ease-readability-formula.php>

Table 1: Privacy policies and terms & conditions: word count, reading time and readability

	Qantas Frequent Flyer	NAB	MyFitnessPal	Westfield WiFi	Woolworths Rewards
Privacy policy					
Word count⁹	6,291	6,027	8,377	6,529	1,814
Reading time¹⁰	22 mins	21 mins	30 mins	23 mins	7 mins
Flesch Reading Ease Formula	39.2/100	45/100	52.9/100	38.1/100	47.5/100
Terms and conditions					
Word count	21,161	37,293	21,250	17,525	8,530
Reading time	73 mins	130 mins	76 mins	62 mins	30 mins
Flesch Reading Ease Formula	31.6/100	55.4/100	43.8/100	43.8/100	58.4/100

Sources: As identified in footnotes and author's calculations.

It is apparent from Table 1 that reading the privacy policy and terms and conditions documents of any of these platforms requires university-level reading skills and, for the terms and conditions, takes more than half an hour—in most cases more than an hour. Few users have the time and the reading skills to seriously scrutinise these documents.

⁹ Roberts (2018) *Word Counter Plus*, <https://chrome.google.com/webstore/detail/word-counter-plus/fpjegfbcdijjkceenlfoehpcakfgldj>

¹⁰ umpox (2017) *Instant Reading Time*, <https://chrome.google.com/webstore/detail/instant-reading-time/afipdkkndmggnmffcmepioemogfnnibf>

I signed up for what?!

What is contained within the privacy policies and terms and conditions of these commonly used digital platforms? They all collect extensive amounts of information, with the intention of using it for advertising or marketing purposes. Common data collection and usage activities are summarised in Table 2 below, with more detail on each platform provided in the following sections.

Table 2: Key terms and conditions and privacy policies of sample sites

	Qantas Frequent Flyer	NAB	MyFitnessPal	Westfield WiFi	Woolworths Rewards
Access to user location?	Yes	Yes	Yes, "precise" location only if user "allows"	Yes	Extent unknown
Access to other sites user looks at?	Yes	Yes	Not specified	Yes	Yes
Provides data analytics to third parties?	Yes	Yes	Yes	Yes	Yes
Collects undefined "other information"?	Not specified	Yes	Yes	Yes	Yes
Access to user social media?	Yes	Yes	Yes	Yes	Yes
Uses 1st/3rd party cookies?	Yes (separate policy)	Yes (separate policy)	Yes	Yes	Yes
Receives user information from third parties?	Yes	Yes	Yes	Yes	Yes
Identifies user device (via IP address, etc.)?	Yes	Yes	Yes	Yes	Implied in Cookies Statement
Can change terms at any time?	Notice given (T&C); Yes (privacy)	Notice given for most (T&C); Yes (privacy)	Revision posted or advanced notice (T&C); Yes (privacy)	Yes	Yes, at any time
Retention of private data?	For as long as necessary	Not specified	For as long as necessary	Indefinitely	Not specified
Can user request data not be used for marketing purposes?	Yes, if contacted	Yes, if contacted	Somewhat	No	Yes for direct marketing, opt out

Qantas Frequent Flyer

Qantas Frequent Flyer terms are spread across several pages: Privacy and Security,¹¹ Qantas Frequent Flyer Terms and Conditions¹² and its Cookies Policy.¹³ Some of these relate only to the Frequent Flyer program whilst others relate to the entirety of Qantas products. It would take an estimated 103 minutes to read these three policies, which total over 29,689 words.

Qantas collects information directly and indirectly from the user. It uses the information it collects on its users for advertising purposes “to generate consumer insights about the Member in order to better understand the Member’s preferences and interests, tailor the Member’s experience, enhance the products and services supplied to the Member ...”¹⁴ In fact, as the Terms and Conditions state: “This is one of the primary purposes of Qantas Frequent Flyer”.¹⁵ The information Qantas uses does not just come from the Member’s direct interactions with Qantas, but also through numerous indirect methods. Qantas combines the data it already has with that of third parties: “... Qantas may collect and combine personal information about the Member from third parties or public sources (e.g. ABS census data)”.¹⁶ This is a broad statement and gives little detail on what personal information is being collected or from where:

... associating and combining data collected from third parties with the Member’s personal information and using and disclosing that combined personal information ... to tailor the Member’s experience and content, including third party content and otherwise in accordance with these Terms and Conditions.¹⁷

By combining data, the advertising the users sees can be incredibly targeted.

NAB

As NAB is a bank, its relationship with the user is a commercial one, where the user’s data is not the product and the reason or partial reason for the platform’s existence (unlike social media platforms or the Qantas Frequent Flyer program). NAB is also obligated to “know its customers” under federal anti-money laundering legislation.¹⁸ Most users would therefore expect data, such as their identification information, credit information and financial details

¹¹ Qantas (2019) *Privacy and Security*, <https://www.qantas.com/au/en/support/privacy-and-security.html#qantas-programs-and-clubs>

¹² Qantas (2019) *Frequent Flyer Terms and Conditions*, <https://www.qantas.com/au/en/frequent-flyer/discover-and-join/terms-and-conditions.html>

¹³ Qantas (n.d.) *Cookies Policy*, <https://www.qantas.com/au/en/support/cookies-policy.html>

¹⁴ Qantas (2019) *Frequent Flyer Terms and Conditions*

¹⁵ Qantas (2019) *Frequent Flyer Terms and Conditions*

¹⁶ Qantas (2019) *Frequent Flyer Terms and Conditions*

¹⁷ Qantas (2019) *Frequent Flyer Terms and Conditions*

¹⁸ National Australia Bank (2019) *Privacy policy*, <https://www.nab.com.au/common/privacy-policy>

to be collected. When using the NAB app or website, information is being collected about users device ID, social media, location, and whether they have accessed third party sites or “other information we think is necessary.”¹⁹ NAB also collects information about users from third parties, including from social media or public registers. Personal information can be used for advertising purposes and:

We may also market our products to you through third party channels (such as social networking sites), or via other companies who assist us to market our products and services. We may use de-identified data to disclose to online advertisers that allow us to place communications in the media most relevant to you.²⁰

The ACCC’s digital platform inquiry found that NAB supplied the advertising firm Quantum with de-identified user transaction data. The ACCC noted that this is not disclosed in NAB’s privacy policy.²¹ From reading the above paragraph, it is not clear what data is being given to advertisers. Users not be concerned by information such as their email being used, but are likely to be more concerned with third parties accessing their spending habits, even if data is anonymous. Like many services, NAB’s language around what specific information is collected and with whom it is shared is vague.

MyFitnessPal

MyFitnessPal is the most used fitness app in Australia and the second most used in the United States.²² Terms and conditions for MyFitnessPal and the wider Under Armour services run across a stunning 938 A4 pages, although this includes considerable repetition and different country and language versions. The word count shown in Table 1 does not cover the entire document—it excludes large sections that are not in English for users in non-English speaking countries.

The app was developed in the United States and has some interesting terms and conditions that would likely constitute unfair contract terms under Australian law. For instance, there is an arbitration clause that prevents a user participating in a class action. This is common in the United States—other companies such as Uber also contain these clauses for its US users:

You acknowledge and agree that you and Uber are each waiving the right to a trial by jury or to participate as a plaintiff or class member in any purported class action or representative proceeding. Unless both you and Uber otherwise agree in writing, any arbitration will be conducted only on an individual basis and not in a class, collective,

¹⁹ National Australia Bank (2019) *Privacy policy*

²⁰ National Australia Bank (2019) *Privacy policy*

²¹ ACCC (2019) *Digital Platforms Inquiry: Final report*, p. 450

²² SimilarWeb (n.d.) *Mobile App Ranking*, <https://www.similarweb.com/apps/top/apple/store-rank/au/health-and-fitness/top-free/iphone>

consolidated, or representative proceeding. However, you and Uber each retain the right to bring an individual action in small claims court and the right to seek injunctive or other equitable relief in a court of competent jurisdiction to prevent the actual or threatened infringement, misappropriation or violation of a party's copyrights, trademarks, trade secrets, patents or other intellectual property rights.²³

This term is likely to be invalid in Australian law.²⁴ The *Competition and Consumer Act 2010* (Cth) states that "a term that limits, or has the effect of limiting, one party's right to sue another party" constitutes an unfair term.²⁵

MyFitnessPal collects data extensively compared to the other platforms analysed in this report:

"**Fitness and Wellness Data**" includes data you provide related to your lifestyle (e.g., sleeping habits), life events, dietary restrictions, fitness goals, height, weight, measurements, fitness level, heart rate, sleep data, BMI, biometric data, and similar types of data relating to physiological condition, and activity. We collect this data in order to provide the Services and to tailor features, products, advertising, and services to your interests and goals, including providing meal suggestions, workout plans, training- and coaching-related services, and product recommendations (e.g., custom products).²⁶

Additionally, the app shares your precise location data with third parties for advertising purposes. If you ever walk past a business and later see an advertisement for that business in your social media feed, you have consented for that level of targeted advertising by using the app. Even if you do not connect the app to your Facebook, the app passively shares information anyway thus allowing social media platforms like Facebook access to your data:

Social network widgets, buttons, and plug-ins on our websites passively transmit data regarding a social network's members to that social network, even when a button is not clicked. These technologies may allow a social network (such as Facebook, Twitter or YouTube) to personally identify its members and to know the web pages its members have visited. This is true wherever social network buttons are embedded, regardless of whether a button is "clicked" or "pressed." If you belong to a social network or use these categories of web services, you should review the privacy policies of those services to understand the nature of the data that they

²³ Noting that, for Uber, the Australian version does not include this clause, but it appears in the US version: Uber (2020) *U.S. Terms of Use*, <https://www.uber.com/legal/en/document/>

²⁴ Bautovich (2018) *Is arbitration innately unfair?*, *mondaq* <https://www.mondaq.com/australia/CorporateCommercial-Law/694380/Is-arbitration-innately-unfair>

²⁵ *Competition and Consumer Act 2010* (Cth), Schedule 2, subsection 25(k), https://www.legislation.gov.au/Details/C2019C00264/Html/Volume_3

²⁶ *Under Armour Privacy Policy* (2018), <https://account.underarmour.com/es-mx/privacy>

collect and what, if any, options the service offers to control how data is collected and used.²⁷

The MyFitnessPal app is an example of the ecosystem that data mining has become. Apps and websites are interconnected—they share the data you give them to create a more complete profile of you.

Westfield WiFi

If you go to a Westfield shopping mall, you can access the free wi-fi. Like many free products on the internet, this is an indication that you are the product rather than the consumer. If you use the free wi-fi, Westfield collects large amounts of personal data, including “but not limited to” your location within their shopping centre, the websites you visit, your device ID, your name and email and the length of your browsing session.²⁸ That is, as much information as though a Westfield employee sat looking over your shoulder at your phone the entire time you browsed. By using the wi-fi, you give Westfield consent to use that information as it wishes:

... for other purposes to which you, either expressly or impliedly, consent to, and for the purposes set out above, we may provide this information to Scentre Group’s agents, contractors, service providers, joint venture and commercial partners and regulatory authorities, and may transfer your personal information to others in countries outside Australia (including to those that operate our cloud servers outside of Australia).

Scentre Group may, for an indefinite period, use the information for the purposes set out above and for promotional, marketing, publicity, research and profiling purposes, including sending electronic messages or push notifications or telephoning users and for such other purposes as set out in our Privacy Policy.²⁹

Westfield also accesses the users’ social media, including your profile picture, contact information, friends list, “and any information you have disclosed in connection with that social media service.”³⁰ There is no option to opt out of this process, by using the wi-fi you accept all aspects of the terms and conditions.

²⁷ *Under Armour Privacy Policy* (2018), <https://account.underarmour.com/es-mx/privacy>

²⁸ Westfield Australia (n.d.) *Wi-Fi Terms of Use and Privacy Terms*, <https://www.westfield.com.au/terms-and-conditions#wi-fi-terms-of-use-and-privacy-terms>

²⁹ Westfield Australia (n.d.) *Wi-Fi Terms of Use and Privacy Terms*

³⁰ Westfield Australia (n.d.) *Wi-Fi Terms of Use and Privacy Terms*

Woolworths Rewards

Woolworths Rewards collects data on a user’s shopping habits and other information for the purpose of targeted advertising. The privacy policy states:

We may also collect personal information about you by accessing data from other sources and then analysing that data together with the information we already hold about you in order to learn more about your likely preferences and interests. When you visit our websites, social media pages or mobile applications or click on our advertisements on the online media of other companies, we may collect information about you using technology which is not apparent to you, for example “cookies”.³¹

It is unclear how much location data the service is collecting. The privacy policy and terms and conditions do not mention location collection. However, if you download the Woolworths app, which allows you to shop online and manage your rewards, the app requests access to your location. Whilst location information may be necessary to shop online, it is unclear if location data is stored or tracked for other reasons. The location information on the Apple App Store indicates that the app collects your location, even when you are not using it, despite that not being an option when consenting for the app to access location.

Figure 3: Woolworths Rewards—consenting to location data

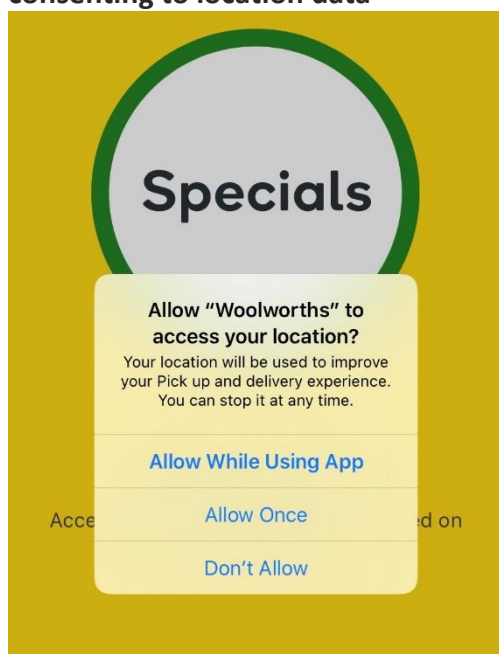


Figure 4: Woolworths Rewards—Apple app Store information

Information	
Seller	Woolworths Group Limited
Size	71.8 MB
Category	Shopping
Compatibility	Works on this iPhone <input type="checkbox"/>
Location	This app may use your location even when it isn't open, which can decrease device battery life.
Languages	English
Age Rating	4+
Copyright	© Woolworths Group Limited 1997-... <input type="checkbox"/>

³¹ Woolworths (2018) *Privacy*, <https://www.woolworthsgroup.com.au/page/privacy-policy>

Conclusion

The collection of user data and its use by digital platforms, which often occurs without the user's knowledge or informed consent, is ubiquitous.

While there is growing awareness of the privacy issues with the large social media and search engine platforms, there is less awareness of the ubiquity of data mining practices between digital platforms and services.

As this report has shown across a number of popular platforms, the difficulty consumers face in reading and understanding their terms and conditions is nearly universal. Most users do not have the time to read these complex legal contracts and understand their implications.

Digital platforms are collecting more data than necessary to perform the supposed primary function of delivering their app or website service. Collection of data is part of a business model whereby the user has become a product themselves.

It is not enough to simply encourage users to read the terms and conditions before they sign up to a service. Even if they did, terms and conditions are predominantly presented on a take it or leave it basis—if the users want the service, they must accept the terms. Stricter rules governing permitted terms in contracts for digital platforms and stronger privacy laws are necessary.